SIP Support in Avaya Communication Manager

Running on the
Avaya S8300, S8400, S8500 series, and
S8700 series Media Server

555-245-206
Issue 7
May 2007

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Copyright

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Contents

About this Document

This document, *SIP Support in Avaya Communication Manager Running on the Avaya S8300, S8400, S8500 series, and S8700 series Media Server*, conveys the following information:

- Explains how to administer Avaya Communication Manager 4.0 to run SES 4.0
- Is a revision of the earlier document of the same name
- Includes corrections and newly developed information

See Avaya Communication Manager documentation for non-SIP issues.

This document is available online and in paper format. For your convenience, consider using the embedded cross-references to locate information in addition to the table of contents and the index. Online readers may also use the search facility of the browser.

Audience

This document is for field technicians, remote service personnel, and user-assigned administrative personnel, as a reference to configure and administer Avaya media servers running Communication Manager with SIP. We recommend having three to five years experience, and experience with working on media servers and Communication Manager.

This document assumes that the engineer has a working knowledge of telecommunication fundamentals and PBX maintenance practices. This document also assumes that the system was initially installed and tested properly and brought into service with every fault cleared. Adjuncts and other devices external to the switch are covered by their own service documentation.

If you do not have these experiences and qualifications, please make arrangements for a mentor.

Document set

Although this book is published separately, it is part of a set. Use this document as an adjunct to the following references:

- *Installing and Administering SIP Enablement Services,* doc ID 03-600768
- *Avaya Communication Manager Administrator Guide*, 03-300509
- *Administration for Network Connectivity for Avaya Communication Manager*, Doc ID 555-233-504

Equipment

The contents of this document discuss the equipment used as media servers running Avaya Communication Manager:

- Avaya S8300
- Avaya S8400
- Avaya S8500 series: S8500 and S8500B and S8500C
- Avaya S8700 series: S8700, S8710, S8720

Organization

- About this Document —What you are reading now gives general information on a SIP implementation, how to use this document, and others.
- Chapter 1: Overview of Changes —This section has high-level information about SIP at a general level that you can read quickly.
- Chapter 2: SIP Support in Avaya Communication Manager—This introduction discusses SIP-related support in general, requirements for SIP, and other related systems.
- Chapter 3: Administering Communication Manager for SIP Enablement Services—Use this section to perform the steps needed to administer Avaya Communication Manager to enable SIP messaging.
- Chapter 4: Communication Manager screen details for SIP—Turn here for detailed descriptions of the screens and fields.

- Appendix A: Requirement specifications—This appendix discusses the compliance requirements for this product and the feature name URIs (FNUs) and how they are implemented in this product.
- Appendix B: Terminal requirements and features—This appendix describes the features and feature interactions for terminals or endpoints.
- Glossary —The glossary provides explanations of abbreviations, acronyms, and terms.
- Index

Conventions

Table 1: Explanation of typography

To represent...	This typeface and syntax are shown as...	For example...
commands	● Bold for **`commands`** ● Bold italic for ***`variables`*** ● Square brackets **[ ]** around optional parameters ● "**|**" between exclusive choices	**`refresh ip-route [all |`** ***`location`*****`]`**
screen input and output	● Bold for **input** ● Constant width for `output (screens and messages)`	Set the `Save Translation` field to **daily**. The message `Command successfully completed` should appear .
Web interface	● Bold for **menu selections, tabs, buttons,** and **field names** ● Right arrow **>** to separate a sequence of menu selections	Select **Alarms and Notification,** the appropriate alarm, and then select **Clear**. Select **Diagnostics > View System Logs**, then select **Watchdog Logs**.
Keys	Special font for **keyboard keys** and SAT screen **clickable buttons**	Press **Tab**. Select **Next Page**.

Other conventions used in this book:

- Physical dimensions are in English units [Foot Pound Second (FPS)], followed by metric units [Centimeter Gram Second (CGS)] in parentheses.

  Wire-gauge measurements are in AWG, followed by the diameter in millimeters in parentheses.
- Circuit-pack codes (such as TN790B or TN2182B) are shown with the minimum acceptable alphabetic suffix (like the “B” in the code TN2182B).

  Generally, an alphabetic suffix higher than that shown is also acceptable. However, not every vintage of either the minimum suffix or a higher suffix code is acceptable. The *Hardware Guide for Avaya Communication Manager,* doc ID 555-245-207, contains current information on circuit pack codes and functionality.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following safety labels and security alert labels:

⚠ **CAUTION:**

A caution statement denotes a situation that can result in harm to software, loss of data, or an interruption in service.

⚠ **WARNING:**

A warning statement indicates a situation that can result in harm to hardware or equipment.

⚠ **DANGER:**

A danger statement alerts you to a situation that can result in harm to personnel.

⚠ **SECURITY ALERT:**

A security alert points to a situation that can increase the potential for unauthorized use of a telecommunications system.

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Related resources

Table 2: Additional document resources, lists additional documentation that is available for you, some of which is referred to within this document.

Table 2: Additional document resources,

Document	Doc ID
4600 Series IP Telephone R2.2 Document Library	16-300091
4600 Series IP Telephone R2.2 Installation Guide	555-233-128
4600 Series IP Telephone R2.2 LAN Administrator's Guide	555-233-507
4602/4602SW SIP Telephone Quick Reference	16-300471
4602/4602SW SIP Telephone User's Guide	16-300470
4610SW SIP Telephone Quick Reference	16-300473
4610SW SIP Telephone User's Guide	16-300472
4620/4621SW SIP Telephone Quick Reference	16-300475
4620/4621SW SIP Telephone User's Guide	16-300474
Administration for Network Connectivity for Avaya Communication Manager	*555-233*-504
Administrator Guide for Avaya Communication Manager	03-300509
Avaya Communication Manager Capacities Table	555-245-601
Avaya Extension to Cellular and OPS Installation and Administration Guide	210-100-500
Avaya Extension to Cellular User's Guide	210-100-700
Avaya Toll Fraud and Security Handbook	555-025-600
Installing and Administering SIP Enablement Services	03-600768
Feature Description and Implementation for Avaya Communication Manager	555-245-205
Hardware Guide for Avaya Communication Manager	555-245-207
Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server	555-234-100
Installing and Configuring the Avaya S8400 Media Server Release	03-300678
Installing and Configuring the Avaya S8500 Media Server	03-300143
	1 of 2

Table 2: Additional document resources, (continued)

Document	Doc ID
Job Aid: Upgrading Firmware on the BIOS — Avaya S8500 Media Server,	03-300411
Job Aids for Field Replacements for the Avaya S8500 Media Server	03-300529
Maintenance Alarms Reference	03-300190
Maintenance Commands Reference	03-300191
Maintenance Procedures	03-300192
online help for Avaya IP Softphone Release 5.x	---
online help for Avaya SIP SoftPhone Release 2.x	---
Quick Start for Hardware Installation Avaya S8400 Media Server in an Avaya G650 Media Gateway	03-300705
Quick Start for Hardware Installation: Avaya S8500 Media Server	555-245-701
Quick Start for Hardware Installation: Avaya S8700 Series Media Server,	555-245-703
Quick Start for Hardware Migration Avaya S8400 Media Server in an Avaya CMC1 or G600 Media Gateway	03-300706
RSA Users Guide	555-245-702
SAMP Users Guide	03-300322
SIP Implementation Guide	16-300140
SIP Personal Information Manager Users Guide	03-300441
SIP Softphone: Administration & System Programming —Avaya SIP Softphone Overview	Aug 2005 Aug 2005
SIP Support for Avaya Communication Manager	555-245-206
The Avaya Server Availability Management Processor (SAMP) User Guide	03-300322
	2 of 2

Technical assistance

Avaya provides the following resources for technical assistance.

- Within the U.S.
- International

Within the U.S.

For help with:

- Feature administration and system applications, call the Technical Consultants System Support group at
  1-800-225-7585
- Maintenance and repair, call the Avaya Remote Technical Services at
  1-800-242-2121
- Toll fraud, call Avaya Technical Services Organization at
  1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Downloading this book from the Web

You can download the latest version of this book from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya web site.

Downloading this book

To download the latest version of this book:

1. Access the Avaya web site at http://support.avaya.com.
2. At the top center of the page, select **Product Documentation**.

   The system displays the **Welcome to Product Documentation** page.
3. In the upper-left corner type the 8- or 9-digit book number in the Search Support field**,** and then select **Go**.

   The system displays the **Product Documentation Search Results** page.
4. Scroll down to find the latest issue number, and then select the book title to the right of the latest issue number.
5. On the next page, scroll down and select one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book in zipped PDF format

Sending us comments

Avaya welcomes your comments about this book.

This document was created in PDF format with commenting enabled. Use Adobe Acrobat v7.0, make your comments and corrections in the PDF file, and send them to us.

To reach us by:

- Mail, send your comments to:

  Avaya Inc.
  Product Documentation Group
  Room B3-H13
  1300 W. 120 Ave.
  Westminster, CO 80234 USA
- E-mail, send your comments to:

  document@avaya.com
- Fax, send your comments to:

  1-303-538-1741

Mention the name and number of this book, *SIP Support in Avaya Communication Manager Running on the Avaya S8300, S8400, S8500 series, and S8700 series Media Server,* (555-245-206, Issue 7).

Chapter 1: Overview of Changes

New and changed information

This section provides links to the new and changed Session Initiated Protocol (SIP) features that affect Communication Manager and Avaya Distributed Office.

- New text for Numbering—Public/Unknown screen on page 57 taken from the Communication Manager administration guide.
- Changed the default for **Session Establishment Timer** field to 3 minutes. This field is in Figure 12: Signaling Group screen, Page 1 on page 67.
- Changed default for **Preferred Minimum Session Refresh Interval** field to be 0. For SIP, the recommended setting remains 1800. See Figure 22: Trunk Group screen, page 2 on page 91
- Added the **Enable Layer 3 Test** field and its discussion on Figure 12: Signaling Group screen, Page 1 on page 67.
- Added the field **Show ANSWERED BY** in Figure 23: Trunk Group screen, page 3 on page 93 screen
- Added material to make SES work with Avaya Distributed Office, particularly on these three screens:
  - ICHT - Incoming Call Handling Treatment screen on page 46
  - Numbering—Public/Unknown screen on page 57
  - ARS/AAR Digit Analysis Table screen on page 39

Chapter 2: SIP Support in Avaya Communication Manager

This chapter describes the support for SIP (Session Initiated Protocol) that is incorporated into Avaya Communication Manager release 4.0, running an Avaya S8300, S8400, S8500 series, or S8700 series media server.

This section contains these major topics:

- Introduction to SIP on page 19
- SIP-related support on page 21
- Requirements for SIP on page 23
- SIP administrative screens on page 37
- SIP device as an OPS extension on page 98

Introduction to SIP

This section introduces SIP for release 4.0 Communication Manager and is divided into two sections:

- What is SIP? on page 19
- How does SIP integrate into your system? on page 20

What is SIP?

SIP is an endpoint-oriented signalling standard that is defined by the Internet Engineering Task Force (IETF). SIP is a text-based protocol based on elements of Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). SIP supports several types of communication sessions that include voice, video, or instant text messaging.

As implemented by Avaya in Communication Manager, SIP trunking functionality is available on the Linux-based S8300, S8400, S8500 series, and S8700 series media servers.

SIP uses an OATS call flow model, in addition to others, and a URI-based feature access extension (Uniform Resource Indicator).

Because SIP-enabled endpoints are managed by Communication Manager, many features can be extended to these endpoints.

The media servers function in three ways:

- As Plain Old Telephone Service (POTS) gateways
- As support for name and number delivery between and among the various non-SIP endpoints that Communication Manager supports. These endpoints can be, for example, analog, Digital Communications Protocol (DCP), or H.323 stations, and analog, digital or Internet Protocol (IP) trunks.
- As support for new SIP-enabled endpoints, such as the Avaya 4620 SIP telephone.

In addition to its calling capabilities, the SIP-enabled release of IP SoftPhone R5 and later, and SIP Softphone R2 and later, includes Instant Messaging (IM) client software, and provides full support for the existing H.323 standard for call control.

How does SIP integrate into your system?

The support for SIP that is built into Avaya Communication Manager is designed to help SIP supplement your present system:

- SIP off loads registrations to SES servers and this improves registration and recovery time of system outages.
- SIP is built around published standards. These standards include both IETF Requests for comments (RFCs) and Internet-Drafts. The standards that the Avaya SIP solution implements include, but are not limited to, these standards:
    - RFC 3261 (SIP)
    - RFC 3265 (SIP Event Notification)
    - RFC 3515 (SIP REFER Method)
    - RFC 3842 (SIP Message Summary and Message Waiting Indication Event Package)
    - RFC 2327 (Session Description Protocol)
    - RFC 3264 (SDP Offer/Answer Model)
    - RFC 2617 (HTTP Digest Authentication)
    - RFC 3325, "*Network Asserted Identity*" is complied with on the SES proxy servers
    - RFC 3891, "*The SIP 'Replaces' Header*"
    - RFC 4028, "*Session Timers in the SIP*"
- SIP integrates with traditional circuit-switched interfaces and IP-switched interfaces. With this integration, the telecommunication system can evolve easily from a circuit-switched telephony infrastructures to next-generation IP infrastructures, including SIP.
- SIP positions customers to leverage, as needed, the increasing number and power of SIP-enabled applications, such as instant messaging and presence.

Note:

> Building SIP support into Communication Manager adds another element to the modular family of Avaya components, which seamlessly delivers a business's voice and messaging capabilities over an IP network. Avaya continues enhancing the value it provides to customers in a standards-based, IP communications infrastructure.

Avaya uses a modular and extensible system architecture to implement SIP support. This architecture has a unique benefit for Avaya customers: the set of features SIP supports is augmented by those features that Communication Manager supports. Any media server that runs a SIP-enabled release of Communication Manager becomes, in effect, a telephony feature server. The Communication Manager media server is accessible from any SIP endpoint and provides access transparently to many telephony features that published SIP standards currently do not address.

SIP-related support

The following sections describe additions made to support SIP in release 4.0 Communication Manager running on the S8300, S8400, S8500 series, and S8700 series media servers media servers:

- Trunking on page 21
- Stations on page 22
- CDR on page 22
- Access control on page 22

Trunking

With support for SIP trunks, an enterprise can connect media servers to a SIP-enabled proxy server, specifically, an Avaya SIP Enablement Services which can then extend to a third-party SIP service provider. The trunk support in Communication Manager complies with SIP standards, specifically IETF RFC 3261, and so interoperates with any SIP-enabled endpoint/ station that also complies with the standard.

In complex configurations with Avaya S8700 series media servers, the signaling-group properties in Communication Manager must be administered to match in certain ways. For more information see SIP trunk engineering notes on page 24.

Stations

Support for SIP stations that use SIP trunks allows any fully compliant SIP telephone to interoperate with Avaya telephones. This means that any SIP telephone, from Avaya or a third party, that complies with the appropriate RFC or Internet-Draft standards can:

- Dial and be dialed as an extension in the enterprise dial plan.
- Put calls on hold and participate in transfers and conference calls.

SIP stations that are administered in Communication Manager as off-PBX station (OPS) stations support most Extended Access features, such as call park, call pick-up, and priority calls. To activate these features, use station buttons set up to dial special extensions, that is, Feature Name Extensions.

For more details, see *Avaya Extension to Cellular User's Guide*, Issue 6, doc ID 210-100-700, and the *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Issue 7, doc ID 210-100-500.

CDR

Avaya provides support for complete call detail records (CDR) for all SIP calls based on the URIs of the calls.

Access control

Avaya provides support for full access control to external trunks from any telephone. Both SIP trunks and SIP endpoints require network access to an Avaya SIP Enablement Services. Note that some other means of access control, such as a firewall, is usually required to control network access from outside the enterprise, that is, to the SES system and through it, to SIP trunks or SIP endpoints inside the enterprise.

Requirements for SIP

The minimum requirements for SIP added to a Communication Manager installation are described in these sections:

- Software on page 23
- Hardware on page 23
- Firmware on page 24
- SIP trunk engineering notes on page 24
- Related systems on page 26

Software

Support for SIP can be enabled in Communication Manager release 4.0 or greater running on any Linux-based media server. The appropriate Avaya remote feature activation (RFA) licensing files are also required.

Hardware

The SIP-enabled release of Communication Manager runs on the following Avaya media servers:

- S8300
- S8400
- S8500 series: S8500 and S8500B
- S8700 series: S8700, S8710, and S8720

Note:

Any of these media servers may also control one or more Avaya media gateways.

All processor ethernet interfaces on S8400 or S8500 hardware, controlled LAN (CLAN) or processor CLAN (procr) IP interfaces must be configured correctly. For more information, see these documents:

Administration for Network Connectivity for Avaya Communication Manager, doc ID 555-233-504

For more information see the *SIP Enablement Services Installation and Administration Guide*, doc ID 555-245-705, Avaya's SIP proxy, endpoint registration and instant messaging server. This product connects to one or several Avaya Communication Manager media servers, and provides SIP-enabled applications such as enterprise instant messaging (IM) that uses the client in Avaya IP SoftPhone R5 or later, or the Avaya SIP SoftPhone R2 or later.

Firmware

Note that SIP standards dictate that dual-tone multi frequency (DTMF) tones be supported within the RTP (Real Time Protocol) data stream. Interoperability with certain third-party, SIP-enabled devices may depend on this. This requirement further demands that the newest releases of Avaya's voice over IP (VoIP) engine be installed throughout your system to support RTP-payload.

For example, any TN2302AP circuit packs that are present in your system must have the most recent firmware version to support DTMF tones within the RTP data stream. Table 3 shows what circuit pack you need for various versions of firmware and hardware.

Table 3: TN2302AP hardware and firmware combinations

	Media Processor	G700/G350/G250 Media Gateway VoIP
Minimum for SIP	V72	V22 or greater
Highly recommended	V93	V93

SIP trunk engineering notes

The SIP signaling group administered on Communication Manager defines the characteristics of a signaling connection.

The total number of calls that can be carried over a single signaling connection is limited by the bandwidth available. There is no true physical trunk when using SIP. Because of this, there is no physical limit on how many calls or trunk members you can set up with a particular signaling connection.

However, using the signaling group and trunk group administrative screens in Communication Manager is also useful for SIP. Doing so extends several Communication Manager features to SIP. Communication Manager normally limits signaling groups to 255 trunk members, limiting each signaling group to 255 calls. For SIP groups, Avaya has removed the restriction that each combination of far-end and near-end IP address/port must be unique for each signaling group. For SIP groups, multiple signaling groups can use the same signaling connections.

More than one signaling group may be administered to share a signaling connection with exactly the same properties of:

- far-end node-name (fe-nn)
- far-end port (fe-pt)
- near-end node-name (ne-nn)
- near-end port (ne-pt).

This kind of administration supports more than 255 calls on the same SIP-based signaling connection, where a signaling connection is defined as <near-end node-name, near-end port, far-end node-name, far-end port>.

For an incoming call, Communication Manager 4.0 compares the caller's domain, as specified in the header of the SIP INVITE message, with the far-end domains specified for the administered SIP signaling groups. If there is a signaling group with a matching far-end domain, that signaling group and its associated trunking resources will be used to handle the incoming SIP call. If there is not a match, then a signaling group with a blank entry for far-end domain will be used. Avaya recommends that at least one SIP signaling group per signaling connection be administered with a blank domain. This blank domain terminates calls from any far-end domains not specifically assigned to other groups. Otherwise, if no matching or blank groups exist, then any SIP signaling group that has trunks available may be used.

All signaling groups that have identical node names/ports, as well as the SIP trunks groups using each of these signaling groups, should be administered with identical properties. That is, fields on this screen should match the analogous fields on the administrative screens.
Of course, different SIP signaling connections will differ with respect to their near-end and/or far-end node names/port numbers, and they *should* have their SIP trunk's signaling groups administered accordingly. It is not appropriate to administer them identically.

In Communication Manager, the number of simultaneous SIP signaling connections is limited to 16. You may administer more than 16, but the run-time limit of simultaneous signaling connections is 16. Remember that a signaling connection is *not* the same as a signaling group, and that more than one SIP signaling group can and should share the same signaling connection.

TLS links for failover

There are 16 available TLS links in SES 3.x and Communication Manager 3.x. For each SIP signaling group administered, when active, it will utilize 1 link on each system (near-end and far-end). In duplexed home server configurations, reserve some TLS links to support failover.

If your configuration is a duplexed SES home server, and some fault occurs that causes a failover to the standby home server, the newly active home server sets up TLS link to the media server running Communication Manager. It might take 15 minutes to bring down the TLS link to the previously active SES Home).

TLS link utilization is real-time. SES and Communication Manager set up TLS links for SIP when they send the very first SIP request, such as INVITE, or SUBSCRIBE/NOTIFY. The link remains active as long as there is SIP message traffic.

Note that the limit of 16 TLS links is a restriction of the Communications Manager.

For example, if you have 10 SIP trunk groups, you have the possibility of a maximum of 10 TLS links in use at one time.

You can have multiple CLANs associated with an SES. With multiple CLANs, you can administer them for load sharing purposes. The Avaya SIP solution does not support alternate CLANs to handle CLAN failure scenarios.

From the SES administrator’s perspective, each SIP endpoint is administered so that it uses one of the available CLANs. If there is an SES home with 3,000 users, and you administer two CLANs to support that SES home, administer 1,500 SIP endpoints to use CLAN #1 and the other 1,500 to use CLAN #2. If CLAN#1 goes down, then those 1,500 SIP endpoints would not be able to make calls. Currently there is no mechanism to administer an alternate CLAN on the SES administration screens.

Related systems

See the *SIP Enablement Services Installation and Administration* document, Issue 2, doc ID 555-245-705, for details on the SIP proxy server.

See the following documentation for details on setting up and using for your Avaya 4600 series SIP telephone as a station for SIP voice calling:

- *4600 series SIP Telephone User’s Guide*, doc ID 16-300035
- *4600 series SIP Telephone Administrator’s Guide*, doc ID 16-300037
- *4600 series SIP Telephone Quick Setup Guide*, doc ID 16-300158
- 4600 Series IP Telephone R2.2 LAN Administrator’s Guide, doc ID 555-233-507
- 4600 Series IP Telephone R2.2 Installation Guide, doc ID 555-233-128
- 4602/4602SW SIP Telephone R2.2 User’s Guide, doc ID 16-300470
- 4602/4602SW SIP Telephone Quick Reference, doc ID 16-3004715
- 4610SW SIP Telephone R2.2 User’s Guide, doc ID 16-300472
- 4610SW SIP Telephone Quick Reference, doc ID 16-300473
- 4620SW/4621SW SIP Telephone R2.2 User’s Guide, doc ID 16-300474
- 4620SW/4621SW SIP Telephone Quick Reference, doc ID 16-300475
- 4600 Series IP Telephone Documentation Library, doc ID 16-300091

For an overview of the different components and the associated tasks that support Avaya’s SIP solution, see the *SIP Implementation Guide*, doc ID 16-300140.

Chapter 3: Administering Communication Manager for SIP Enablement Services

This chapter describes the screens to visit and the fields to change so that your SES and Communication Manager system can run SIP trunks to the SES.

For detailed information and rationale about these steps, see these sections:

- SIP administrative screens on page 37
- SIP device as an OPS extension on page 98

Administering Communication Manager for SIP

This section describes how to administer and configure SIP on a Communication Manager system so that Communication Manager can support SIP endpoints. You administer and configure the system with Communication Manager screens, some of which are specific to SIP.

You may have been directed to this point from the section in the SES installation procedures, from the section, *Administering Communication Manager and endpoints.* All installation work discussed prior to this point should be correctly completed.

Communication Manager must function properly before you start SIP administration. If your Communication Manager installation uses the Enhanced Meet Me conferencing feature, install that feature before you start the following administration steps.

Administer SIP endpoints on Communication Manager using OPS. OPS gives you advanced SIP telephony.

To administer SIP trunks in Communication Manager 4.0, complete the procedures in this section. Each step includes a link to an example screen if you need it.

- Prepare Communication Manager on page 28
- Administer SIP trunks on page 31
- Administer call routing on page 33
- Redirect calls off the network on page 35

Prepare Communication Manager

Complete these steps to prepare Communication Manager for SES.

1. Verify that your system supports and is correctly configured for IP connectivity.

   See *Administration for Network Connectivity for Avaya Communication Manager*, doc ID 555-233-504.

2. Go to the **System Capacity** screen.

   Figure 14: System Capacity screen on page 74.

   Check the values for the field **SIP Trunks (included in "Trunk ports"**).

   If no values are displayed here, it means that your SIP has not been licensed properly. You cannot proceed. Correct SIP licensing problems and begin here after that.

3. Go to the **System-Parameters Customer-Options screen page 4**.

   Figure 19: System Parameters Customer Options screen, page 4 **on page 81**.

   Check the following values:

   a. Set the field **ISDN PRI** to **y**.

   b. Verify that the **IP Trunks** field is set to **y**.

   c. Set the field Enhanced **EC500** to y.

   You must log off and log back in to effect changes to System Parameters Customer-Options screens.

4. Go to the **System Parameters Customer-Options screen page 2**.

   Figure 18: System Parameters Customer Options screen, page 2 on page 80

   Verify that the **Maximum Administered SIP Trunks** field has a value within these ranges:

   - 0 through 400 for S8300 servers
   - 0 through 500 for S8400 servers
   - 0 through 800 for S8500 servers
   - 0 through 5000 for S8700/S8710/S8720 servers

   You must log off and log back in to effect changes to System Parameters Customer-Options screens.

5. Go to the **System Parameters Customer Options screen, page**. **1**

   Figure 17: System Parameters Customer Options screen, page 1 on page 78.

   Use these fields at the bottom:

   - **Maximum Off-PBX Telephones - EC500, for cell phones**
   - **Maximum Off-PBX Telephones - OPS, for advanced SIP telephony phones**

   In each field, enter the number of stations that you want to set up for each type of Off-PBX telephone.

   You must log off and log back in to effect changes to System Parameters Customer-Options screens.

6. Go to the **IP Node Names screen**.

   Figure 6: IP Node Names screen **on page 54**.

   Check all fields to make sure that they are correct for your network.

7. Go to the **IP Address Mapping** screen.

   Figure 4: IP Network Map screen **on page 48**.

   Enter the IP address and the host name for the administered SES server on your network in the corresponding fields.

8. Go to the **IP Network Region screen** to assign an IP network region for the SIP trunk.

   Figure 5: IP Network Region screen **on page 50**.

   a. In the **Authoritative Domain** field, enter the SIP domain name for which this network region applies. This same SIP domain name is used in the SES interface.

   b. Set the field **Intra-region IP-IP Direct Audio** to y.

   c. Set the field **Inter-region IP-IP Direct Audio** to y

   d. Set the field **Server IP Address** to the to the IP address of the RTCP Monitor server.

   e. Set the field **Server Port** to the RTCP Monitor server.

9. Go to the **Signaling Group screen page 1**.

   Figure 12: Signaling Group screen, Page 1 on page 67.

   a. Type **sip** in the field **Group Type**. The system displays a screen for SIP groups.

   b. Verify that the **Transport Method** field contains the default value of **tls**.

   c. In the **Near-end Node Name** field, type the name of the IP interface at the near (local) end of the SIP trunk signaling group.

      For the S8300, S8400, or S8500 media server, the value of this entry is typically **procr**.

      For an S8700 series media server, the entry is the **node name** for the selected CLAN or procr interface.

d. In the **Far-end Node Name** field, enter the name of the node that you administered as the SIP proxy server in Step 6.

e. In the **Near-End Listen Port** field, type the recommended TLS port value of **5061**.

f. In the **Far-end Listen Port** field, type the recommended TLS port value of **5061**.

g. For the **Far-end Network Region** field, if you want the SIP proxy server that you administered in Step 6 to use the codec set and/or parameters specified for an IP network region to be different from that of the LAN IP interface, then enter the region of the SIP proxy.

h. In the field **DTMF over IP**, make sure that the value is **rtp-payload**.

i. The recommended value for the field **SIP Session Establishment Timer** is 3 minutes.

j. Setting the field **Enable Layer 3** Test is optional. The default is **n**. The value **n** uses the ping test and does not use the OPTIONS test. Enter a **y** to use the OPTIONS test instead of a ping.

Administer SIP trunks

Use these steps to set up SIP trunks on Communication Manager.

1. Go to the **System Parameters Features screen page 1**.

   Figure 15: System Parameters Feature screen Page 1 **on page 76**.

   a. Set the **DID/Tie/ISDN/SIP Intercept Treatment** field to **attd**.

   b. Verify that the **Trunk-to-Trunk Transfer** field is set to **restricted**.

2. Go to the **Trunk Group screen page 1**.

   Figure 21: Trunk Group screen, page 1 on page 83:

   a. Type **sip** in the **Group Type** field.

   The screen displays fields that pertain to for SIP groups. An entry of **sip** also affects the fields that are presented on other administrative screens discussed later.

   b. Depending on your need for call detail recording, type **y** for yes or **n** for no in the **CDR Reports** field.

   Note that very large numbers of CDR reports may be generated by SIP calls.

   c. Type the number of the SIP signaling group that you previously administered in the **Signaling Group** field.

   d. Type a value of 0 through 255 in the **Number of Members** field for the number of SIP trunks that belongs to this group.

   Group Member Assignments are automatically completed and populated on the Trunk Group screens **on page 83**, and on any subsequent pages that are necessary, based on the values that you entered on the **Trunk Group screens**. Group members cannot be administered individually. All members of each administered group share the same characteristics.

   Note:

   The total number of all SIP trunks that are specified for all groups must be less than or equal to the value in the **Maximum Administered SIP Trunks** field on the **System-Parameters Customer Options** screen. For more information, see Figure 14: System Capacity screen on page 74.

   e. Repeat the preceding Steps a. through d. for each SIP trunk group you want to assign, up to your media server's trunk-number limit.

3. Go to the Trunk Group screen, Page 2 on page 91.

   Set the field **Group type** to **sip**.

   Administer the other fields on this screen as necessary for your system.

4. Go to the **Trunk Group screen page 3**.

   Trunk Group screen, page 3 on page 93.

   Verify that the value in the **Numbering Format** field is what you want, Public, Private, unk-pvt, or Unknown.

   Administer the other fields on this screen as necessary for your system.

5. Go to the **Trunk Group screen page 4**.

   Trunk Group screen, page 4 on page 97.

   Set the field **Mark Users as Phone?** to **y** for a particular trunk *only* if a device or a network that is connected to that SIP trunk requires the **User as Phone** parameter. Set to y if a public network trunks through a SIP service provider.

6. Go to the **Numbering - Public/Unknown Numbering screen** and assign public unknown numbering data.

   If your SES installation is part of an Avaya Distributed Office network, this screen should match extensions, trunks, and prefixes in Avaya Distributed Office Central Manager.

   See the Numbering—Public/Unknown screen on page 57.

7. Go to the **Station screen page 1**.

   See the Station screen page 1 on page 73.

   Set the field **Type** to 46xx, where xx is the ending digits of your station type. If you use 46xx as the Type, the system generates minor alarms for these stations. You may ignore these alarms.

   If you set **Type** to DCP, undesirable interactions with the TTI and other features may occur.

8. Go to the **Configuration Set screen page 1**.

   Figure 2: Configuration Set screen on page 44.

   Set the field **Configuration Set Description** to **SIP phone**.

9. Go to the **Off-pbx Station Mapping screen** page 1.

   Figure 9: Off-pbx station mapping screen page 1 on page 58.

   Add station mapping data for SIP endpoints.

10. Go to the **Off-pbx Station Mapping screen** page 2.

    Figure 10: Off-pbx station mapping screen page 2 on page 62.

    Add station mapping data for SIP endpoints.

Administer call routing

Before you can make SIP calls from endpoints that are connected to Communication Manager, administer call routing properly in Communication Manager.

1. Go to the **Feature Access Code** screen.

   Feature Access Codes screen page 1 on page 45.

   You may set either the ARS Access code fields, or the AAR Access code fields or both. To enable these fields, make sure that on the **System Parameters Customer Options** screen page 5, the **Private Networking** field is set to **y**. See Figure 20: System Parameters Customer Options screen, page 5 on page 82.

2. Go to the **ARS Digit Analysis Table** screen.

   Figure 1: ARS Digit Analysis Table screen on page 39.

   Administer this screen to make sure that dialed strings of digits are interpreted correctly and the resulting calls are routed appropriately using the SIP trunks that you administered in Step 2 through Step 5 in the section Administer SIP trunks on page 31.

   Note:

   > You may not access a SIP trunk with a dialed TAC.

   If you use Avaya Distributed Office, you must administer this screen to use AAR. Avaya Distributed Office does not use ARS.

3. Go to the **Route Pattern** screen.

   Figure 11: Route Pattern screen **on page 65**.

   Verify that the **Secure SIP** field is set to the default value of **n** for routing through a public network.

   You can set **Secure SIP** to **y** only if you have a secure connection between the public SIP network and the SES home server that you are routing to.

   Choose a route pattern. Fill in the correct trunk, FRL, and number of digits to insert and delete.

   Perform this task using either AAR or ARS. The most frequent case would be for ARS.

4. Go the **Numbering-Public/Unknown Numbering** screen.

   Figure 8: Numbering—Public/Unknown screen **on page 57**.

   Make an entry here for the trunk that you use in your route pattern.

   For Avaya Distributed Office, confirm that the value for **Ext Len** matches what is specified in the field **SES Edge 4.0**.

5. Go to the **Locations** screen.

   Figure 7: Locations screen **on page 56**.

   Type the appropriate **Proxy Selection Route Pattern** in the field that corresponds to each location employing a SIP proxy server.

6. Go to the **IP Network Map** screen.

   Figure 4: IP Network Map screen **on page 48**.

   Use the **IP Network Map** screen to allow the system to identify the location of a caller who dials a 911 emergency call from a SIP endpoint. For more information on this topic, see the *Screen Reference* chapter in the *Avaya Communication Manager Administrator Guide*, 03-300509.

   a. Use the **`ip-network map`** command to go to the IP Address Mapping screen and map emergency calls.

      SIP endpoint users can move from place to place. A roaming SIP user can be unregistered at one location and moved to another location when they log in to a SIP phone.

      To ensure that SIP phones send the correct emergency number, enter the range (**From IP Address** and **To IP Address**) of your SIP phones in the IP Address Mapping screen.

   b. Use the **`ip-network map`** command to go to the IP Network Map screen.

   c. In the **Emergency Location Extension** field, enter the extension number that you want your SIP telephones to send to the public Safety Answering Point, for example, 911@company.com.

      This extension number will be prepended by your entry in the Public Numbering table for the trunk that you use. If you have several locations, make multiple entries in the IP Addressing Map screen. Each entry requires an emergency location extension.

7. If you are installing Avaya Distributed Office, make sure that the dial plan is correct for incoming calls.

   Go the Incoming Call Handling Treatment screen and make sure that this screen reflects the correct branch prefixes. Use the command **`change inc-call-handling-trmt trunk-group`** ***`n`***, where n is a valid trunk group number.

   The field **Incoming Call Handling Treatment** specifies call handling for ISDN and SIP Enablement Services (SES) trunk groups.

Redirect calls off the network

You might want to do additional administration to direct the coverage of calls that are redirected off the network (CCRON).

Communication Manger monitors the progress of calls from inception to conclusion. If calls go off net, Communication Manger will never recognize the call as completed. Because of the virtual nature of SIP trunks, set this field to **n** to enable call classification over interworked trunks.

Go to the **System Parameters—Call Coverage/Call Forwarding screen**.

Figure 16: System Parameters—Call Coverage/Call Forwarding screen on page 77.

Set the field **Disable Call Classifier for CCRON over SIP trunks** to **y** or **n**, depending on your system.

For SIP, this field is usually set to **n**.

Chapter 4: Communication Manager screen details for SIP

This section contains examples of properly populated screens that you might need to check as you administer Communication Manager for SIP trunking.

Best Practices

- When you add a SIP station in Communication Manager, use DCP set types that can be X-ported. This prevents excessive alarming caused by using 46xx set types.

  If you use 46xx station types, you receive minor alarms for these stations. You may ignore these alarms.

  If you use DCP station types, some undesirable interactions occur with the TTI and other features. Some trunk types do not allow TTI'ed X-ported stations, like SBS trunks, to call over them.
- When you add the SIP station in Communication Manager, *do not* use 4602 or 2402 set types. Even the 4602 SIP telephone needs at least three call appearances to handle conference and transfer operations.
- Similarly, on the **change off-pbx-telephone station-mapping x** screen page 2, the **Call Limit** should be at least **3**, but also should match what the telephone has if the telephone has more than 3 call appearances (default is **2**).

SIP administrative screens

This section explains how to administer the following Communication Manager screens to support SIP trunking:

- ARS/AAR Digit Analysis Table screen on page 39
- Configuration Set screen on page 44
- Feature Access Codes screen page 1 on page 45
- Incoming Call Handling Treatment screen on page 46
- IP Network Map screen on page 48
- IP Network Region screen on page 50
- IP Node Names screen on page 54

- Locations screen on page 56
- Numbering—Public/Unknown screen on page 57
- Off-PBX Station Mapping screen page 1 on page 58
- Off-PBX Station Mapping screen page 2 on page 62
- Route Pattern screen on page 65
- Signaling Group Page 1 screen on page 67
- Station screen, page 1 on page 73
- System Capacity screen on page 74
- System-Parameters screens on page 75
- SIP device as an OPS extension on page 98
- Trunk Group screens on page 83

These screens deal with SIP administration. Every effort, when possible, has been made to put correct field values in the screen examples. Look at them carefully.

Only SIP-related screens are described in this document. In all instances of screens and table descriptions, see the *Administration for Network Connectivity for Avaya Communication Manager* and the *Avaya Communication Manager Administrator Guide*, 03-300509, for more details about all Avaya Communication Manager screens and fields, including the SIP-related ones presented here.

Other screens that might require your attention are found on SIP device as an OPS extension on page 98. The features and the configuration of your SES SIP network determine what you administer on these screens. See SIP device as an OPS extension on page 98.

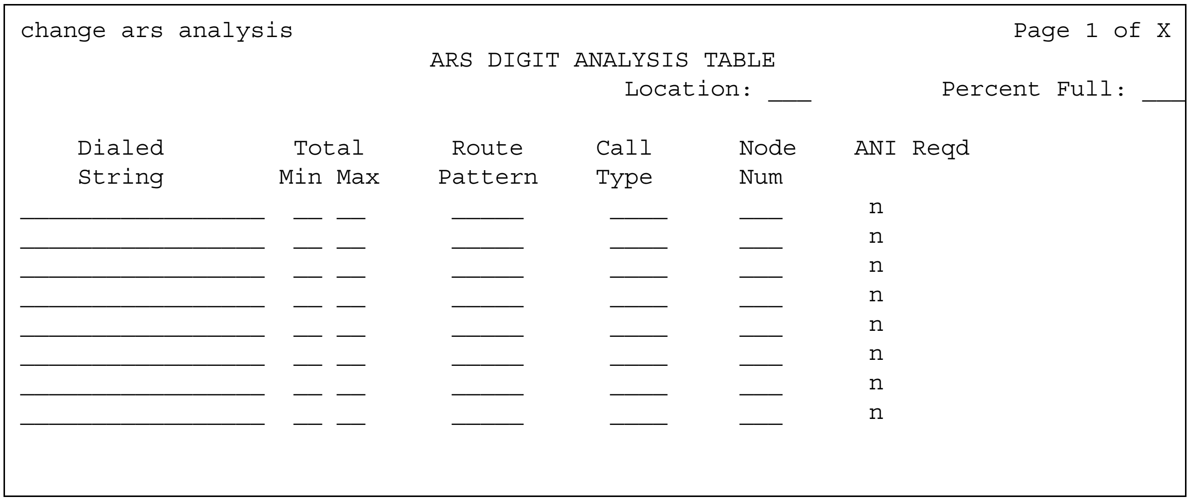
ARS/AAR Digit Analysis Table screen

Communication Manager compares dialed numbers with the dialed strings in this table and determines the route pattern for the number.

If you alter data in this table, resynchronize data as described in the document *Installing and Administering SES*, the section titled Data Synchronization between Communication Manager and PPM. The SIP-related fields are in bold in this screen.

If your SIP installation is part of Avaya Distributed Office, complete this screen with **AAR** as the value in the Call Type field. Avaya Distributed Office does not use ARS.

Figure 1: ARS Digit Analysis Table screen



```
change ars analysis                                                   Page 1 of X
                            ARS DIGIT ANALYSIS TABLE
                                         Location: ___        Percent Full: ___

    Dialed         Total       Route     Call      Node    ANI Reqd
    String        Min Max     Pattern    Type      Num
_________________  __ __       _____      ____      ___      n
_________________  __ __       _____      ____      ___      n
_________________  __ __       _____      ____      ___      n
_________________  __ __       _____      ____      ___      n
_________________  __ __       _____      ____      ___      n
_________________  __ __       _____      ____      ___      n
_________________  __ __       _____      ____      ___      n
_________________  __ __       _____      ____      ___      n
```

ANI Reqd

Valid entries	Usage
y/n	Enter **y** if ANI is required on incoming R2-MFC or Russian MF ANI calls. This field applies only if the **Request Incoming ANI (non-AAR/ARS)** field on the **Multifrequency-Signaling-Related System Parameters** screen is **n**.
r	Allowed only if the **Allow ANI Restriction on AAR/ARS** field on the **Feature Related System Parameters** screen is **y**. Use to drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails. Other types of trunks treat **r** as **y**.

Call Type (for AAR only)

In this field in the ARS Digit Analysis Table screen, enter the call type that is associated with each dialed string. Call types indicate numbering requirements on different trunk networks. ISDN protocols are listed in the table below.

Valid entries	Usage
aar	Regular AAR calls.
intl	The Route Index contains public network ISDN trunks that require international type of number encodings.
pubu	The Route Index contains public network ISDN trunks that require international type of number encodings.
lev0 to lev2	Specify ISDN Private Numbering Plan (PNP) number formats.

ISDN Protocol

Call Type	Numbering Plan Identifier	Type of Numbering
aar	E.164(1)	national(2)
intl	E.164(1)	international(1)
pubu	E.164(1)	unknown(0)
lev0	PNP(9)	local(4)
lev1	PNP(9)	Regional Level 1 (2)
lev2	PNP(9)	Regional Level 2 (1)

Call Type (for ARS only)

Valid entries	Usage	Usage in China #1
alrt	Alerts attendant consoles or other digital telephones when an emergency call is placed	normal
emer	emergency call	normal
fnpa	10-digit North American Numbering Plan (NANP) call (11 digits with Prefix Digit "1")	attendant
hnpa	7-digit NANP call	normal
intl	public-network international number	toll-auto
iop	international operator	attendant
locl	public-network local number	normal
lpvt	local private	normal
natl	non-NANP	normal
npvt	national private	normal
nsvc	national service	normal
op	operator	attendant
pubu	public-network number (E.164)-unknown	normal
svcl	national(2)	toll-auto
svct	national(2)	normal
svft	service call, first party control	local
svfl	service call, first party control	toll

Dialed String

In the ARS Digit Analysis Table screen, user-dialed numbers are matched to the dialed string entry that most closely matches the dialed number. For example, if a user dials 297-1234 and the AAR or ARS Digit Analysis Table has dialed string entries of 297-1 and 297-123, the match is on the 297-123 entry.

An exact match is made on a user-dialed number and dialed string entries with wildcard characters and an equal number of digits. For example, if a user dials 424, and there is a 424 entry and an X24 entry, the match is on the 424 entry.

Valid entries	Usage
0 to 9	Enter up to 18 digits that the call-processing server analyzes.
***, x, X**	Wildcard characters

Location (for the ARS Digit Analysis Table)

This is a display-only field on the ARS Digit Analysis Table screen shown in the ARS Digit Analysis Table screen.

Valid entries	Usage
1 to 64	Defines the location of the server running Avaya Communication Manager that uses this ARS Digit Analysis Table. On the System-Parameters Customer-Options screen, the ARS field and the Multiple Locations field must be set to **y** for values other than **all** to appear.
all	Indicates that this ARS Digit Analysis Table is the default for all port network (cabinet) locations. Appears only if the Multiple Locations field is set to **n** on the System-Parameters Customer-Options screen.

Max

In the ARS Digit Analysis Table screen, this is appears as the Total Max field.

Valid entries	Usage
Between **Min** and **28**	Enter the maximum number of user-dialed digits the system collects to match to the dialed string.

Min

In the ARS Digit Analysis Table screen, this appears as the Total Min field.

Valid entries	Usage
1 to **Max**	Enter the minimum number of user-dialed digits that the system collects to match to the dialed string.

Node Num

In the ARS Digit Analysis Table screen, enter the number of the node.

Valid entries	Usage
1 to **999** or blank	Enter the number of the destination node in a private network if you use node number routing or FCS. If you complete this field, leave the **Route Index** field blank.

Percent Full

This field in the ARS Digit Analysis Table screen, displays the percentage (0 to 100) of system memory resources that have been used by AAR/ARS. If the figure is close to 100%, you can free memory resources.

Route Pattern

In this field in the ARS Digit Analysis Table screen, enter the route number that you want the server running Avaya Communication Manager to use for this dialed string.

Valid entries	Usage
p1 to **p2000**	Specifies the route index number established on the Partition Routing Table.
1 to **640**	Specifies the route patterns used route the call.
1 to **999**	Specifies the route pattern used to route the call. For S8300 media server only.
r1 to **r32**	Specifies the remote home numbering plan area (RHPNA) table. Complete this field if RHNPA translations are required for the corresponding dialed string.
node	Designates node number routing.
deny	Block the call.

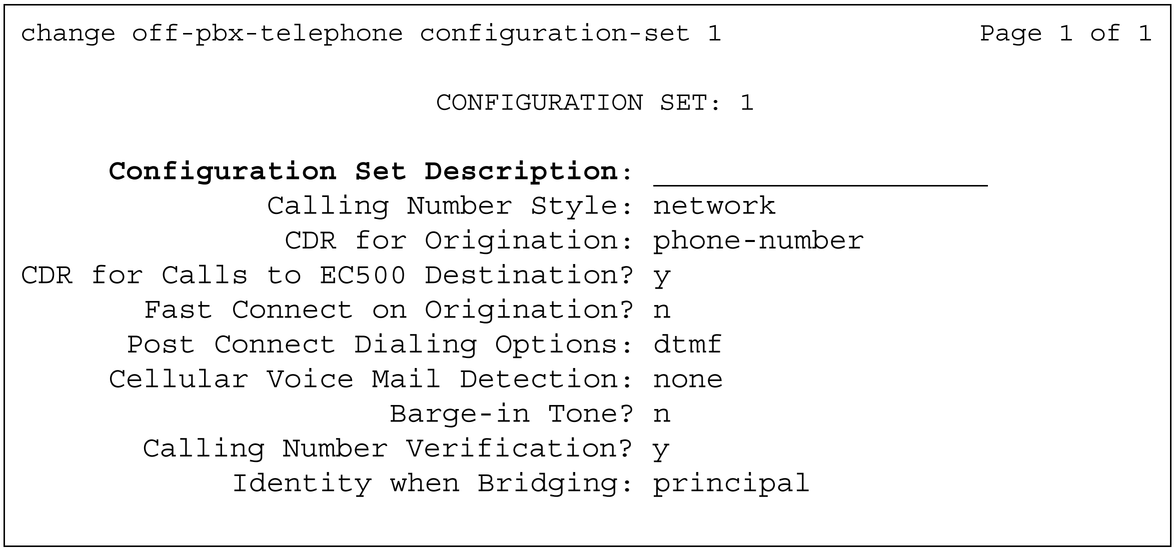
Configuration Set screen

This screen defines a several call treatment options for EC500 cell phone calls. The EC500 allows the use of up to 10 Configuration Sets, which are already defined in the system with default values.

For SIP, set the field **Configuration Set Description** to **SIP Phone**. Complete the other fields to meet the needs of your SIP endpoints.

The SIP-related fields are in bold in this screen.

Figure 2: Configuration Set screen



```
change off-pbx-telephone configuration-set 1              Page 1 of 1

                        CONFIGURATION SET: 1

     Configuration Set Description: ____________________
              Calling Number Style: network
               CDR for Origination: phone-number
CDR for Calls to EC500 Destination? y
       Fast Connect on Origination? n
      Post Connect Dialing Options: dtmf
     Cellular Voice Mail Detection: none
                     Barge-in Tone? n
       Calling Number Verification? y
            Identity when Bridging: principal
```

Configuration Set Description

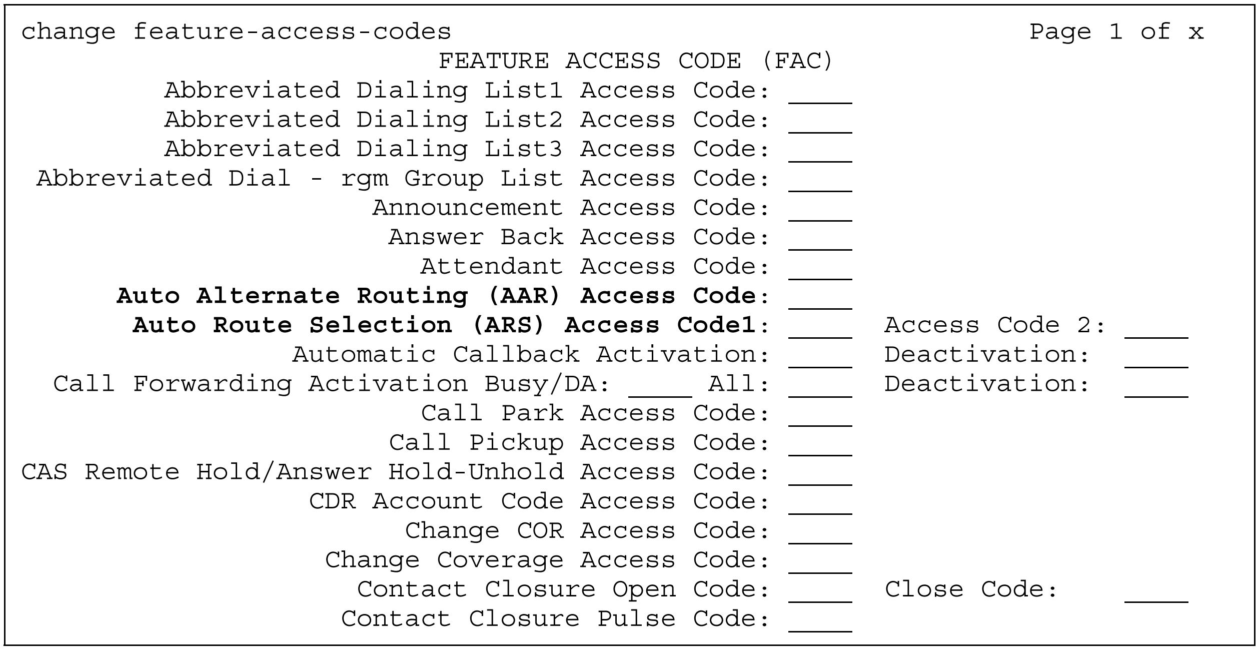
Describes the purpose of the configuration set.

Valid entries	Usage
Up to 20 alphanumeric characters or blank	For example, EC500 handsets. For SIP, enter **SIP Phone**.

Feature Access Codes screen page 1

This screen assigns feature access codes (FACs) that, when dialed, activate or cancel the system features. Each field on this screen has the same valid values, which must conform to feature access codes or dial access codes as defined by your dial plan.

The SIP-related fields are in bold.



```
change feature-access-codes                                    Page 1 of x
                          FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
 Abbreviated Dial - rgm Group List Access Code: ____
                      Announcement Access Code: ____
                       Answer Back Access Code: ____
                         Attendant Access Code: ____
      Auto Alternate Routing (AAR) Access Code: ____
       Auto Route Selection (ARS) Access Code1: ____  Access Code 2: ____
                 Automatic Callback Activation: ____  Deactivation:  ____
  Call Forwarding Activation Busy/DA: ____ All: ____  Deactivation:  ____
                         Call Park Access Code: ____
                       Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
                  CDR Account Code Access Code: ____
                        Change COR Access Code: ____
                   Change Coverage Access Code: ____
                     Contact Closure Open Code: ____  Close Code:    ____
                    Contact Closure Pulse Code: ____
```

Auto Alternate Routing (AAR) Access Code

Use this field to access AAR.

Auto Route Selection (ARS) Access Code1

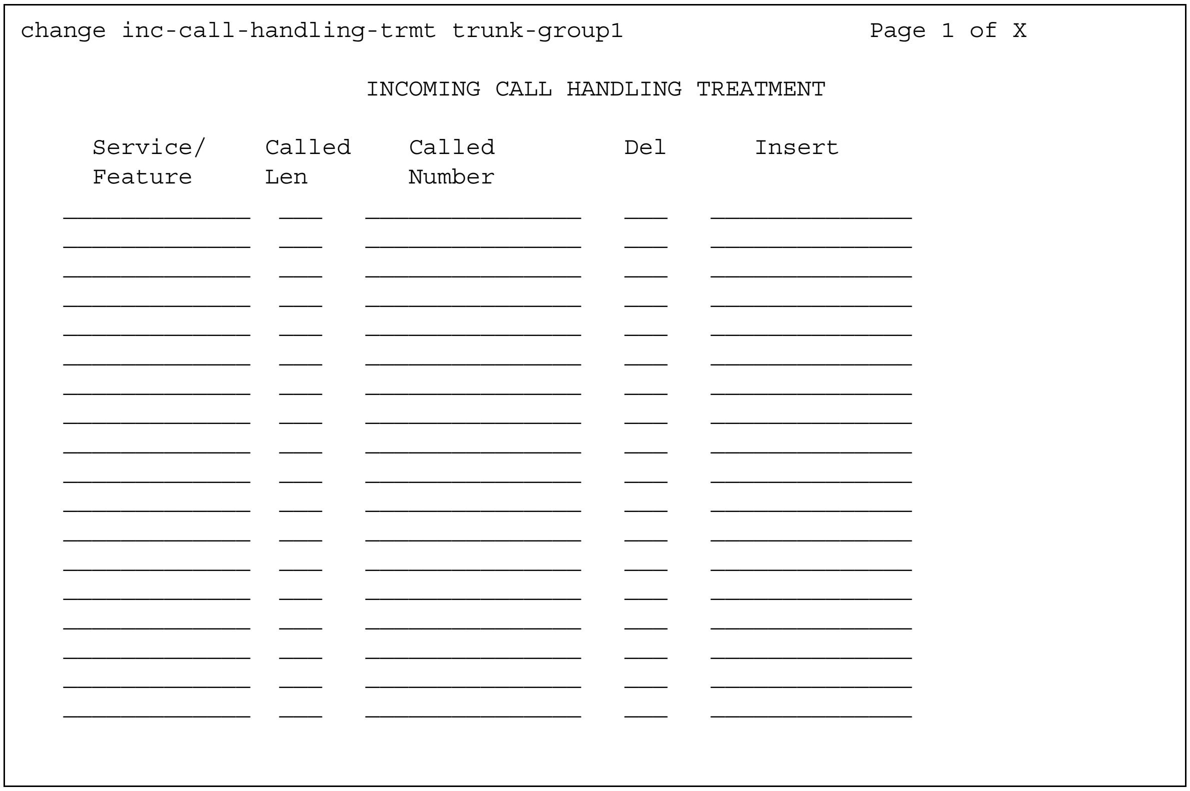
Use this field to access ARS. You can have one ARS access code for local and one code for long distance, and route accordingly.

Incoming Call Handling Treatment screen

For SIP Enablement Services (SES) trunk groups, the **Per Call CPN/BN** and **Night Serv** fields do not appear because these fields do on a screen for ISDN trunks.

The SIP-related fields are in bold in this screen.

Figure 3: Incoming Call Handling Treatment screen



```
change inc-call-handling-trmt trunk-group1                 Page 1 of X

                        INCOMING CALL HANDLING TREATMENT

     Service/    Called    Called         Del      Insert
     Feature     Len       Number

   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
   _____________  ___   _______________   ___   ______________
```

Called Len

The Called Len field in the Incoming Call Handling Treatment screen specifies the number of digits received for an incoming call. A blank entry may be used only for the situation in which the **Called Number** field has been set to blank. When used with the blank entry, this means that any length of digits associated with the Called Party IE of the Incoming SETUP message will match this field. The use of the **0** entry is encouraged for the situation in which the PSTN provider does not provide any 'Number Digits' within the received Called Party IE (such as in Japan). Valid entries are **0** to **21**, or leave blank.

Called Number

The Called Number field in the Incoming Call Handling Treatment screen specifies the leading digits received for an incoming call. A blank entry is used as a "wild card" entry and, when used, means that any number associated with the specified Service/Feature can match in this field. Valid entries are up to 16 digits, or leave blank.

Del

The Del field in the Incoming Call Handling Treatment screen specifies the number of leading digits to be deleted from the incoming Called Party Number. Calls of a particular type can be administered to be routed to a single destination by deleting all incoming digits and then administering the **Insert** field with the desired extension. Valid entries are **1** to **21**, **all**, or leave blank.

Insert

The Insert field in the Incoming Call Handling Treatment screen specifies the digits to be prepended to the front of the remaining digits after any (optional) digit deletion has been performed. The resultant number formed from digit deletion/insertion is used to route the call, provided night service is not in effect. Valid entries are up to 16 characters consisting of a combination from the following: **0** to **9**, *****, **#**, or leave blank.

Service/Feature

This field in the Incoming Call Handling Treatment screen is display-only. It is auto-populated with the value entered in the **Service Type** field on the **Trunk Group** screen.

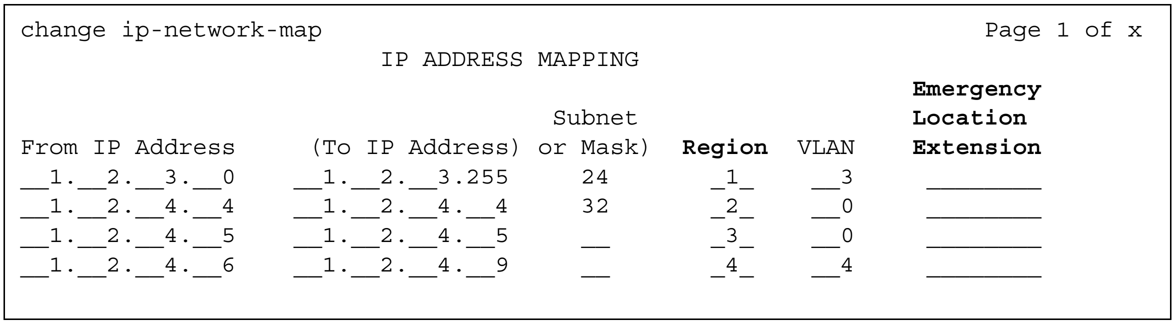
IP Network Map screen

The **IP Address Mapping** screen in Figure 4 shows the SIP-related information in bold.

You must administer this screen *only* if you use Emergency Contacts as part of your SES system.

If you alter data in this table, resynchronize data as described in *Installing and Administering SES*, the section titled Data Synchronization between Communication Manager and PPM.

Figure 4: IP Network Map screen



```
change ip-network-map                                                  Page 1 of x
                         IP ADDRESS MAPPING
                                                                   Emergency
                                           Subnet                  Location
From IP Address      (To IP Address)  or Mask)  Region   VLAN      Extension
__1.__2.__3.__0     __1.__2.__3.255     24        _1_     __3       ________
__1.__2.__4.__4     __1.__2.__4.__4     32        _2_     __0       ________
__1.__2.__4.__5     __1.__2.__4.__5     __        _3_     __0       ________
__1.__2.__4.__6     __1.__2.__4.__9     __        _4_     __4       ________
```

Note:

In release 4.0 of Communication Manager, use this screen to allocate resources for both H.323 and SIP endpoints.

The IP Address Mapping screen for 911 calls allows you to have a range of IP addresses in a location. You can then assign a 911 number that will be sent to the Public Safety Answering Point (PSAP) if any of the phones within that range of 911 IP addresses makes an emergency call.

You can also have another range of addresses for another location with an assigned 911 number.

If a user in one location moves to the second location, and makes an emergency call, the user's endpoint sends the correct CPN to the PSAP. Without using the ip-network-map, each SIP station sends out it own number if it makes an emergency call.

This step is important in distributed Communication Manager environments in which network bandwidth may be consumed unnecessarily for calls among SIP and other endpoints.

Region

This field in the IP Network Map screen identifies the network region for the IP address range. Make sure the Region value you set here reflects the Authoritative Region on screen IP Network Region screen on page 50.

If this screen does not correlate with the IP Network Region screen correctly, calls will not be processed successfully. Communication Manager may not assume its authoritative role for the call and routes back out to the proxy. The proxy then redirects back to Communication Manager. In the **Locations** form shown on page 56, the **proxy sel. rte. pat.** field causes the call to route out to the proxy. But if this were not configured, the call would be rejected with a 403 Screening Failure.

For SIP, the setting for Region must be the same as the Region field in the IP Network Region screen on page 50.

Valid entries	Usage
1 to 250	The network region number for this interface. This field must contain a non-blank value if the **From IP Address** field on the same row contains a non-blank value.

Emergency Location Extension

This field in the IP Network Map screen allows the system to properly identify the location of a caller who dials a 911 emergency call from this station. An entry in this field must be of an extension type included in the dial plan, but does not have to be an extension on the local system. It can be a UDP extension. The entry defaults to blank. A blank entry typically would be used for an IP softphone dialing in through PPP from somewhere outside your network.

If you populate the IP Address Mapping screen with emergency numbers, the feature functions as follows:

- If the Emergency Location Extension field in the Station screen is the same as the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension to the Public Safety Answering Point (PSAP).
- If the Emergency Location Extension field in the Station screen is different from the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension in the IP Address Mapping screen to the Public Safety Answering Point (PSAP).

Valid entries	Usage
0 to 9 (up to 7 digits)	Enter the emergency location extension for this station. Default is blank.

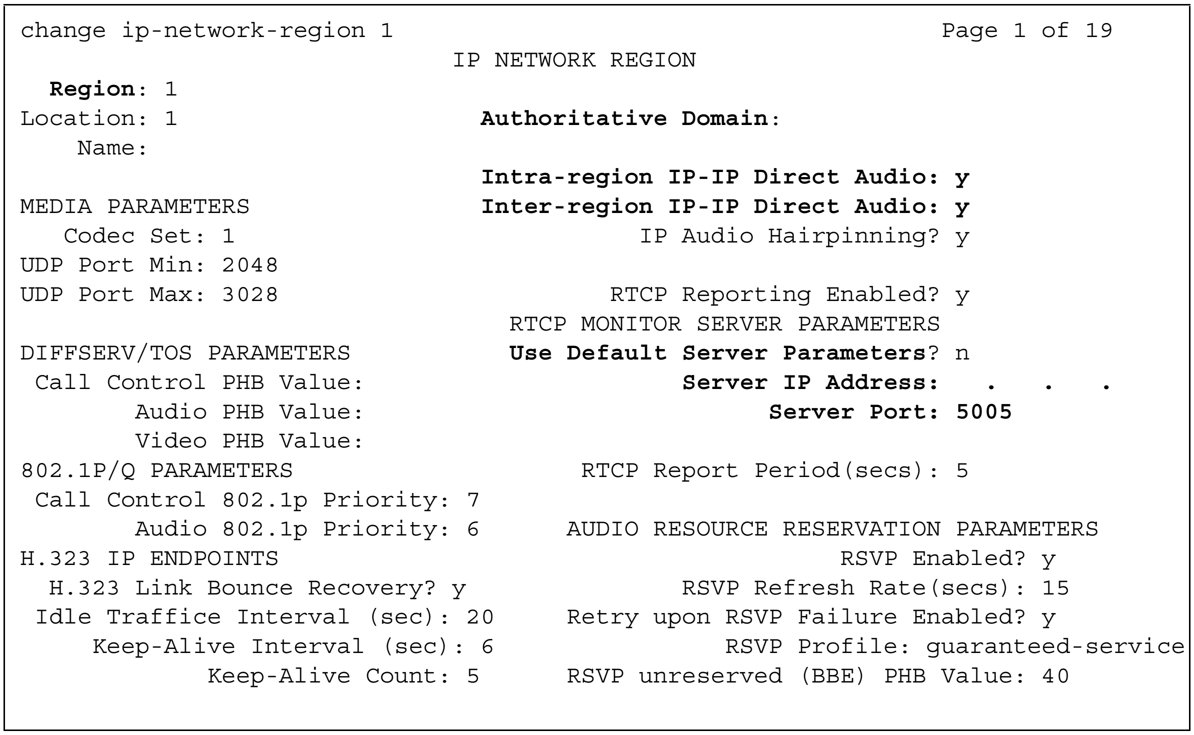
Note:

On the ARS Digit Analysis Table screen, you must administer 911 to be call type emer or alrt in order for the E911 Emergency feature to work properly.

IP Network Region screen

The SIP-related fields are in bold in this screen.

Figure 5: IP Network Region screen



```
change ip-network-region 1                                      Page 1 of 19
                              IP NETWORK REGION
  Region: 1
Location: 1                     Authoritative Domain:
    Name:
                                Intra-region IP-IP Direct Audio: y
MEDIA PARAMETERS                Inter-region IP-IP Direct Audio: y
   Codec Set: 1                            IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3028                       RTCP Reporting Enabled? y
                                  RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS           Use Default Server Parameters? n
 Call Control PHB Value:                      Server IP Address:   .   .   .
        Audio PHB Value:                            Server Port: 5005
        Video PHB Value:
802.1P/Q PARAMETERS                    RTCP Report Period(secs): 5
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? y
  H.323 Link Bounce Recovery? y               RSVP Refresh Rate(secs): 15
 Idle Traffice Interval (sec): 20     Retry upon RSVP Failure Enabled? y
     Keep-Alive Interval (sec): 6                RSVP Profile: guaranteed-service
             Keep-Alive Count: 5      RSVP unreserved (BBE) PHB Value: 40
```

Region

You can change the properties of each region administered in the IP Network Map screen on page 48 using this screen.

Authoritative Domain

The **Authoritative Domain** field in the IP Network Region screen must be set to the same value as the SIP domain administered, the home domain, or a third-party proxy for the signaling group associated with this network region.

This field designates the name or IP address of the domain for which this network region is responsible or authoritative.

Valid entries	Usage
Up to 20 characters or blank.	Enter the name or IP address of the domain for which this network region is responsible. Note that this will appear in the From header of any SIP messages.

A valid entry in this field is required for SIP endpoints on Communication Manager to call the public network.

Note that the value for this Authoritative Domain field must match the content of the Domain field on the Edit screen in SES, which is set with the Master Administration web interface in the SES system.

In a single-server configuration, a home authoritative server combined on an Edge server, exactly one authoritative domain is set, for example, *company.com*.

In a duplex configuration, each home is subject to the domain to which it is connected. Each Edge can have a separate domain, and a single CM can support multiple domains.

Subdomains are not supported. You may not use domain structures such as *eastcompany. com* or *westcompany.com.*

Intra-region IP-IP Direct Audio

Set this field in the IP Network Region screen to **n** to prevent direct audio connections between IP endpoints within a network region. Usually a SIP installation sets this to **y**.

Valid entries	Usage
y/n	Enter **y** to save on bandwidth resources and improve sound quality of voice over IP transmissions. An **n** entry might be used if, for example, the IP phones within the region are behind two or more fire walls.

Valid entries	Usage
native(NAT)	Enter **native(NAT)** if the IP address from which audio is to be received for direct IP-to-IP connections within the region is that of the telephone/softphone itself (without being translated by NAT). IP phones must be configured behind a NAT device *before* this entry is enabled.
translated(NAT)	Enter **translated(NAT)** if the IP address from which audio is to be received for direct IP-to-IP connections within the region is to be the one with which a NAT device replaces the native address. IP phones must be configured behind a NAT device before this entry is enabled.

Inter-region IP-IP Direct Audio

This field in the IP Network Region screen allows direct audio connections between IP endpoints within a network region.

For SIP, set this to **n**. In SIP, band width is virtual. See SIP trunk engineering notes on page 24.

Valid entries	Usage
y/n	Enter **y** to save on bandwidth resources and improve sound quality of voice over IP transmissions. An **n** entry might be used if, for example, the IP telephones within the region are behind two or more fire walls.
native(NAT)	Enter **native(NAT)** if the IP address from which audio is to be received for direct IP-to-IP connections within the region is that of the telephone/softphone itself (without being translated by NAT). IP phones must be configured behind a NAT device before this entry is enabled.
trnslated(NAT)	Enter **translated(NAT)** if the IP address from which audio is to be received for direct IP-to-IP connections within the region is to be the one with which a NAT device replaces the native address. IP phones must be configured behind a NAT device before this entry is enabled.

Use Default Server Parameters

Set this field in the IP Network Region screen to **n** so that the screen displays the fields **Server IP address** and **Server Port**.

Server IP Address

The system displays this field, as shown in the IP Network Region screen, only when the **Use Default Server Parameters** field is set to n and the and the **RTCP Enabled** field is set to y.

For SIP, set this field to the IP address of the RTCP Monitor server.

Valid entries	Usage
0 to **255** in a series of four octets.	Enter the IP address for the RTCP Monitor server

Server Port

The system displays this field, as shown in the IP Network Region screen, only when the **Use Default Server Parameters** field is set to n and the **RTCP Enabled** field is set to y.

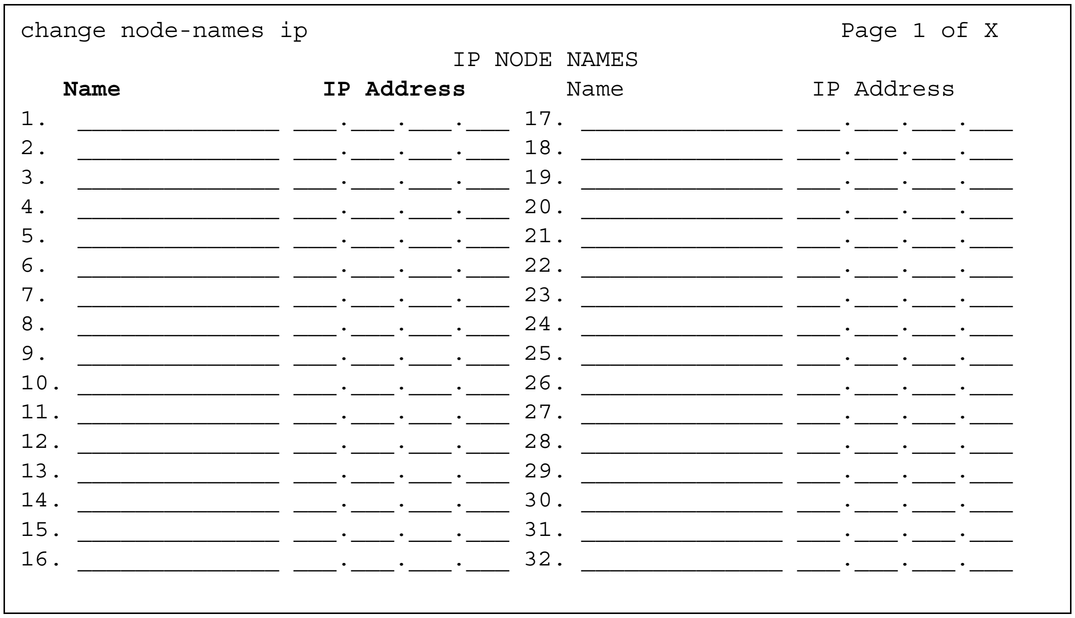
Valid entries	Usage
1 to **65535**	Enter the port number for the RTCP Monitor server.

IP Node Names screen

Enter the friendly names and the IP addresses for SES home servers and CLAN or procr on this screen.

The SIP-related fields are in bold in this screen.

Figure 6: IP Node Names screen



```
change node-names ip                                          Page  1 of  X
                                IP NODE NAMES
   Name                  IP Address         Name                 IP Address
1.   _______________ ___.___.___.___ 17.  _______________ ___.___.___.___
2.   _______________ ___.___.___.___ 18.  _______________ ___.___.___.___
3.   _______________ ___.___.___.___ 19.  _______________ ___.___.___.___
4.   _______________ ___.___.___.___ 20.  _______________ ___.___.___.___
5.   _______________ ___.___.___.___ 21.  _______________ ___.___.___.___
6.   _______________ ___.___.___.___ 22.  _______________ ___.___.___.___
7.   _______________ ___.___.___.___ 23.  _______________ ___.___.___.___
8.   _______________ ___.___.___.___ 24.  _______________ ___.___.___.___
9.   _______________ ___.___.___.___ 25.  _______________ ___.___.___.___
10.  _______________ ___.___.___.___ 26.  _______________ ___.___.___.___
11.  _______________ ___.___.___.___ 27.  _______________ ___.___.___.___
12.  _______________ ___.___.___.___ 28.  _______________ ___.___.___.___
13.  _______________ ___.___.___.___ 29.  _______________ ___.___.___.___
14.  _______________ ___.___.___.___ 30.  _______________ ___.___.___.___
15.  _______________ ___.___.___.___ 31.  _______________ ___.___.___.___
16.  _______________ ___.___.___.___ 32.  _______________ ___.___.___.___
```

Note:

If you are using an SES system for SIP, enter the IP address for the SIP Proxy Server, a home or home/edge, for your network in the corresponding fields.

Name

The **Name** column in the IP Node Names screen identifies the name of an adjunct or server, or switch node.

Valid entries	Usage
1 to 15 alphanumeric characters	Used as a label for the associated IP address. The node names must be unique for each server and switch.

IP Address

The **IP Address** column in the IP Node Names screen identifies for the node named in the previous field by it's dotted octet address.

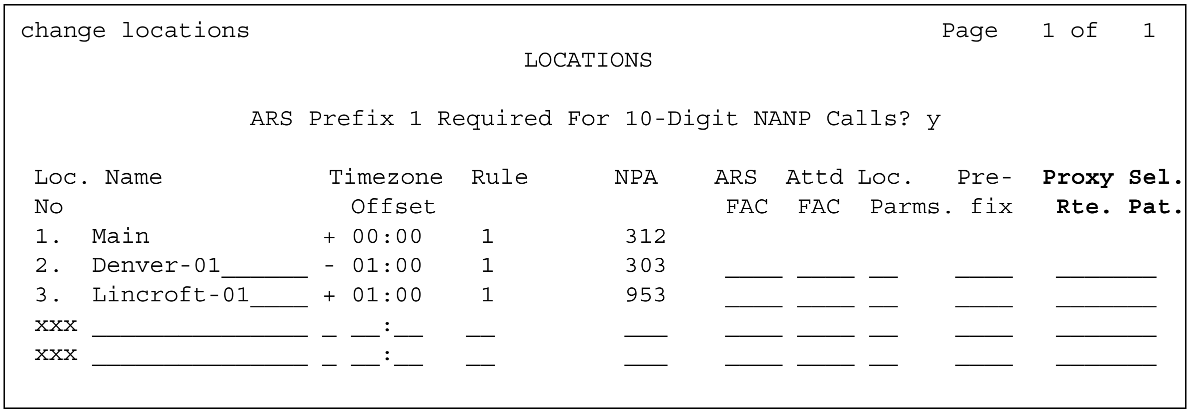
Valid entries	Usage
32-bit address (4 decimal numbers, each in the range 0 to 255)	A unique IP address is assigned to each port on any IP device that is used for a connection. See the *Administration for Network Connectivity for Avaya Communication Manager*, doc ID 555-233-504 for more information.

Locations screen

This screen allows for each location to point to the route pattern that is routing to its outbound SIP proxy server. This correlation is required by features and services such as Transfer and URI Dialing. You may use any route pattern for any SIP trunk.

The SIP-related fields are in bold.

Figure 7: Locations screen



```
change locations                                                Page   1 of   1
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc. Name           Timezone  Rule      NPA    ARS  Attd Loc.   Pre-  Proxy Sel.
 No                    Offset                    FAC  FAC  Parms. fix   Rte. Pat.
 1.  Main            + 00:00    1         312
 2.  Denver-01______ - 01:00    1         303    ____ ____ __    ____   _______
 3.  Lincroft-01____ + 01:00    1         953    ____ ____ __    ____   _______
 xxx _______________ _ __:__   __         ___    ____ ____ __    ____   _______
 xxx _______________ _ __:__   __         ___    ____ ____ __    ____   _______
```

Proxy Selection Route Pattern

The Proxy Selection Route Pattern field identifies the routing pattern that leads to the proxy server. This is the route pattern assigned on the **Route Pattern** screen.

Valid entries	Usage
1 to **999** or blank	Type the number of the routing pattern to be used to get to the proxy server.

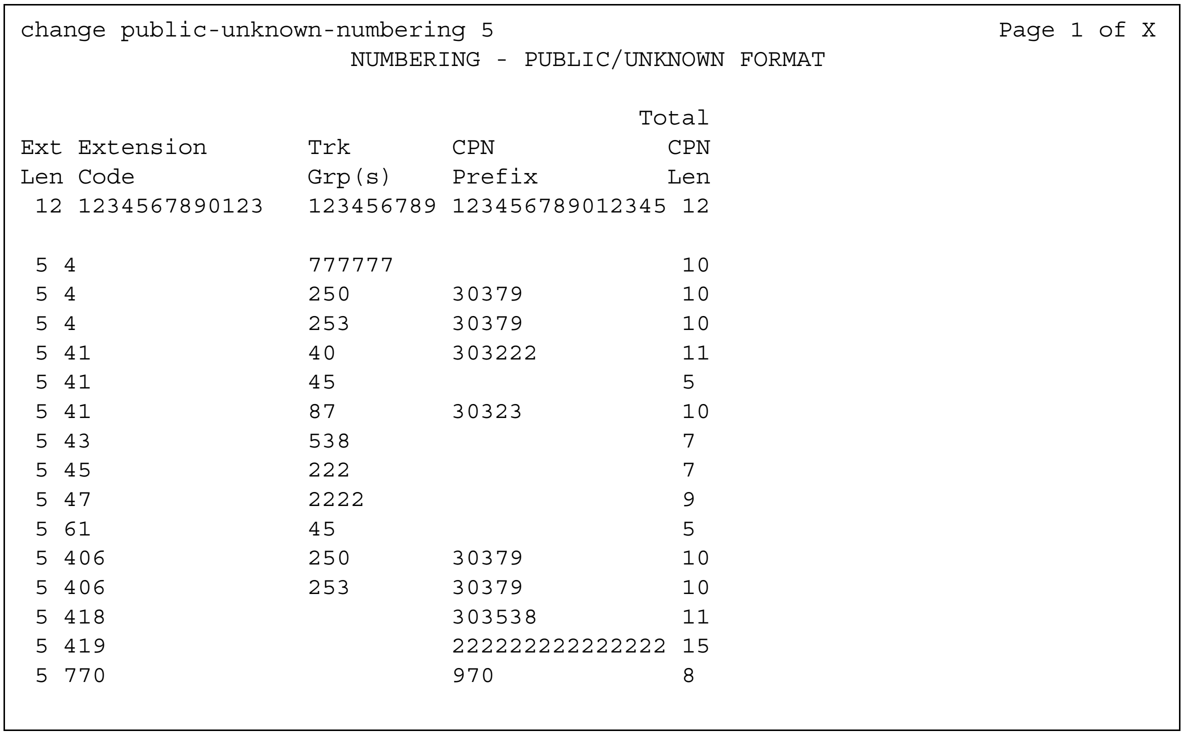
Numbering—Public/Unknown screen

Access the **Numbering — Public/Unknown** screen with the command **`change public-unknown-numbering`** ***`n`***, where ***`n`*** is the length of a value between **0** and **7** appearing in the **Ext Code** column.

The screen consists of two pages: page 1 displays up to 30 **Ext Code** entries matching the requested **Ext Code** length entered on the command line, and page 2 provides 30 blank entries for new user input. If there is sufficient room on the screen, **Ext Code** entries that are longer than the specified length are also displayed. Enter a length of **0** to designate the attendant. If there are more entries of length ***`n`*** than can be displayed, modify your command to use the **`ext-digits`** ***`x`*** command line modifier. For Avaya Distributed Office, confirm that the value for **Ext Len** matches what is specified in the field **SES Edge 4.0**.

The SIP-related fields are in bold in this screen.

Figure 8: Numbering—Public/Unknown screen



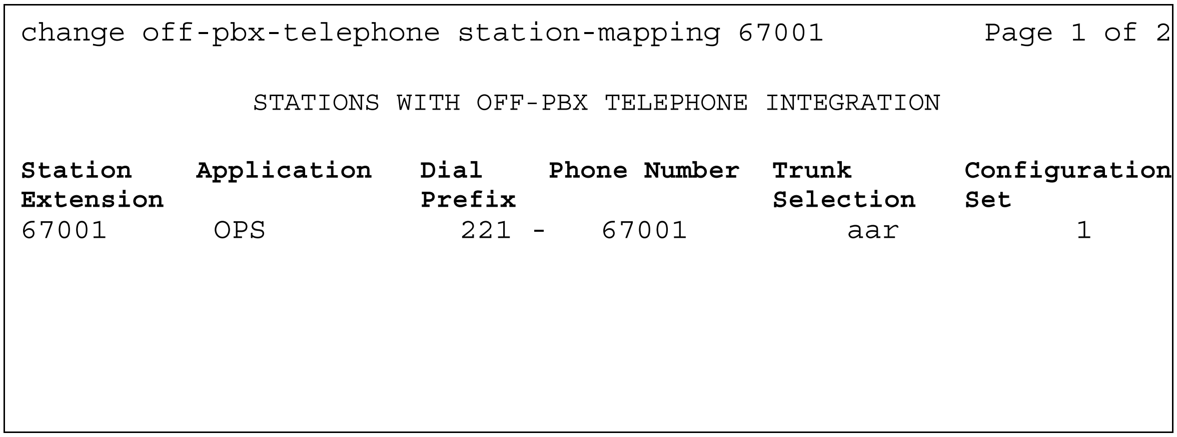
```
change public-unknown-numbering 5                                 Page 1 of X
                       NUMBERING - PUBLIC/UNKNOWN FORMAT

                                           Total
Ext Extension       Trk       CPN            CPN
Len Code            Grp(s)    Prefix         Len
 12 1234567890123   123456789 123456789012345 12

 5 4                777777                   10
 5 4                250       30379          10
 5 4                253       30379          10
 5 41               40        303222         11
 5 41               45                       5
 5 41               87        30323          10
 5 43               538                      7
 5 45               222                      7
 5 47               2222                     9
 5 61               45                       5
 5 406              250       30379          10
 5 406              253       30379          10
 5 418                        303538         11
 5 419                        222222222222222 15
 5 770                        970            8
```

Off-PBX Station Mapping screen page 1

Use the Stations with Off-PBX Telephone Integration screen to map an office phone to a cell phone through the Extension to Cellular feature. The office phone can be a standard office number or an administration without hardware (AWOH) station. For more information on Extension to Cellular, see *Feature Description and Implementation for Avaya Communication Manager*, 555-245-205.

This screen relates to the System-Parameters Customer-Options screen, page 1 on page 78.

Figure 9: Off-pbx station mapping screen page 1



```
change off-pbx-telephone station-mapping 67001         Page 1 of 2

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station    Application   Dial    Phone Number  Trunk      Configuration
Extension                Prefix                Selection  Set
67001       OPS            221 -    67001          aar           1
```

Command parameters

Action	Object	Qualifier
add	off-pbx-telephone station-mapping	
change	off-pbx-telephone station-mapping	<station extension>
display	off-pbx-telephone station-mapping	<station extension>
list	off-pbx-telephone station-mapping	<variable>

The `add off-pbx-telephone station-mapping` command displays the blank Stations with Off-PBX Integration screens. You can add up to sixteen associations between an office telephone and an external telephone.

The `change off-pbx-telephone station-mapping <station extension>` command displays the Stations with Off-PBX Integration screens. You can change the associations between office telephones and external telephones. The first line on the screen contains the information for the station extension that you entered as the command variable. You can also add additional associations in this screen.

The `display off-pbx-telephone station-mapping <station extension>` command displays the **Stations with Off-PBX Integration** screens. The `<station extension>` variable is optional. These screens list up to sixteen entries, starting with the station extension you entered as the command variable. If this extension is not administered for an off-PBX, the display starts with the next administered off-PBX extension in numerical order.

The `list off-pbx-telephone station-mapping <variable>` command information about the association between an office phone and an off-PBX phone. The command variable specifies the office phone number or numbers of interest. The `<variable>` can be:

- A complete phone number
- A partial phone number followed by an asterisk, which is a “wildcard” character
- Blank

Station Extension

The Station Extension field in the Off-pbx station mapping screen page 1 is an administered extension in your dial plan. This number is the extension of the office telephone.

Valid entries	Usage
A valid number in your dial plan	Type an extension number of the office phone up to eight digits. Default is blank.

Application

In the Off-pbx station mapping screen page 1, indicate the type of off-PBX application that is associated with the office phone. You can assign more than one application to an office phone.

Valid entries	Usage
blank	Default is blank.
EC500	Cell phone with Extension to Cellular
OPS	SIP-enabled phone
CSP	Cell phone with Extension to Cellular provided by the cellular service provider

Dial Prefix

The system prepends the Dial Prefix to the off-PBX phone number before dialing the off-PBX phone. The system deletes the dial prefix when a user enters their cell phone number using the Self Administration Feature (SAFE) access code. You must set the routing tables properly so that the dial prefix "1" is not necessary for correct routing. See Figure 9, the Off-pbx station mapping screen page 1.

Valid entries	Usage
blank **0** through **9, *, #**	Type up to four digits, including “*” or “#”. If included, “*” or “#” must be in the first digit position. Enter a "1" if the phone number is long-distance. Enter "011" if the phone number is international. Default is blank.

Phone Number

Enter the phone number of the off-PBX phone in this field in the Off-pbx station mapping screen page 1.

Valid entries	Usage
0 through **9**	Type up to fifteen digits. Enter the complete 10-digit number. Default is blank.

Trunk Selection

The Trunk Selection field in the Off-pbx station mapping screen page 1 defines which trunk group you will use for outgoing calls.

Valid entries	Usage
ars **aar** **trunk group number**	Indicate which trunk group to use for outgoing calls.

Configuration Set

Use the **Configuration Set** field in the Off-pbx station mapping screen page 1 to administer the Configuration Set number. This number contains the desired call treatment options for the station. Ninety-nine Configuration Sets exist.

Valid entries	Usage
1 through **99** **blank**	Type the number of the Configuration set or sets. Default is blank

Dial Prefix

The system prepends the Dial Prefix to the off-PBX phone number before dialing the off-PBX phone. The system deletes the dial prefix when a user enters their cell phone number using the Self Administration Feature (SAFE) access code. You must set the routing tables properly so that the dial prefix "1" is not necessary for correct routing. See Figure 9: Off-pbx station mapping screen page 1.

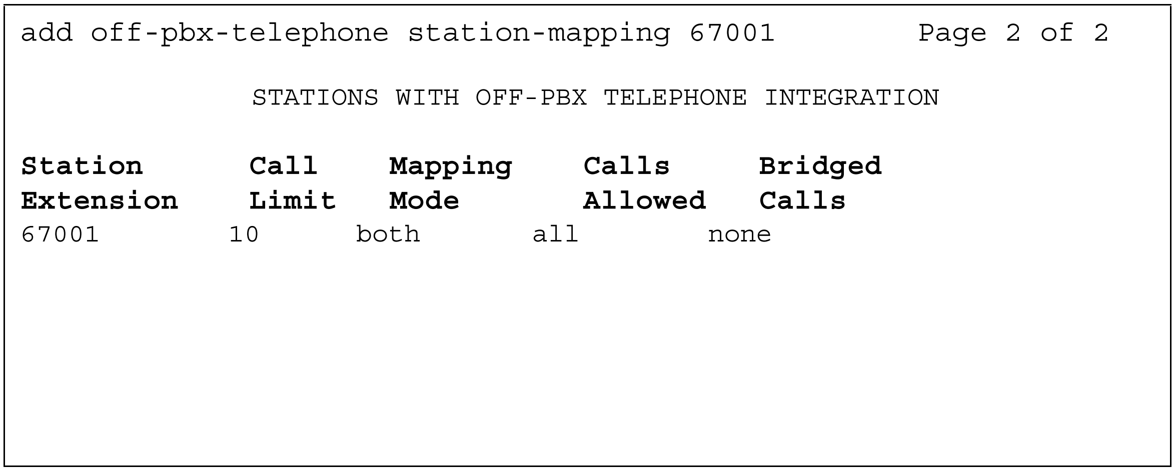
Valid entries	Usage
blank **0** through **9, *, #**	Type up to four digits, including “*” or “#”. If included, “*” or “#” must be in the first digit position. Enter a "1" if the phone number is long-distance. Enter "011" if the phone number is international. Default is blank.

Off-PBX Station Mapping screen page 2

Finish the administration steps to map an office phone to an off-PBX phone on the second page of the **Stations with Off-PBX Telephone Integration** screen. The information you entered in the first page appears as read-only information on the second page.

The SIP-related fields are in bold in this screen.

Figure 10: Off-pbx station mapping screen page 2



```
add off-pbx-telephone station-mapping 67001        Page 2 of 2

                STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station         Call    Mapping     Calls      Bridged
Extension       Limit   Mode        Allowed    Calls
67001          10      both        all        none
```

Station Extension

The Station Extension field is an administered extension in your dial plan. This number is the extension of the office phone. See the Off-pbx station mapping screen page 2 above.

Valid entries	Usage
a valid number in your dial plan	Type an extension number of the office phone up to eight digits. Default is blank.

Call Limit

The Call Limit field in the Off-pbx station mapping screen page 2 sets the maximum number of simultaneous calls.

Valid entries	Usage
blank **1** through **10**	Set the maximum number of calls that can be active simultaneously. Default is 2.

Mapping Mode

Enter the mode of operation for the Extension to Cellular cell phone. Use these modes to control the degree of integration between the cell phone and the office phone. The modes are valid for calls only. For each office phone, you can only assign one cell phone as the origination mode. You cannot assign a cell phone as either the origination or both mode more than once. See Figure 10: Off-pbx station mapping screen page 2.

Valid entries	Usage
both	Default is **both** when the Phone Number field was previously administered for another extension with a Mapping Mode of termination or none. Default = termination when the Phone Number field was previously administered with a Mapping Mode of origination or both. In the both mode, users can originate and receive calls from the office phone with the cell phone.
termination	In termination mode, users can only use their cell phone to receive calls from the associated office phone. Users cannot use the cell phone to originate calls from the associated office phone. Calls originating from the cell phone independent of the office phone are independent of Extension to Cellular and behave exactly as before enabling Extension to Cellular.
origination	In origination mode, users can only originate cell phone calls from the associated office phone. Users cannot use the cell phone to receive calls from the associated office phone.
none	In the none mode, users cannot originate or receive calls from the office phone with the cell phone.

Calls Allowed

Identifies the call filter type for a station. The Calls Allowed values filter the type of calls to the office phone that a user can receive on a cell phone. See Figure 10: Off-pbx station mapping screen page 2.

Valid entries	Usage
all	Default is **all**. The cell phone receives both internal and external calls.
internal	The cell phone receives only internal calls.
external	The cell phone receives only external calls.
none	The cell phone does not receive any calls made to the associated office phone.

Bridged Calls

Use the Bridged Calls field to determine if bridged call appearances extend to the cell phone. The valid entry definitions are the same as the Mapping Mode field entries. See Figure 10, the Off-pbx station mapping screen page 2.

Valid entries	Usage
both	Default is **both**.
termination	
origination	
none	For OPS, which SIP often is, you must use **none**. This enables bridged appearances on OPS phones to work correctly.

Configuration considerations for SIP phones

The Bridged Calls field should be set to **none** unless the SIP station supports the Avaya extensions for bridged appearances. If this field has a value other than **none**, a call to your SIP station goes immediately to coverage without ringing if another SIP phone that is *not* registered has a bridged appearance on your phone.

Avaya 4600-series SIP Telephones will not be able to register in an SES system unless they can obtain the correct SIPDOMAIN setting from the *46XXsettings.txt* file. Always configure the SIPDOMAIN setting for the phones in the file named *46XXsettings.txt* file and then ensure that the phones transfer settings from the file (via tftp or http) during boot up. The line in the file for this setting is:

```
SET SIPDOMAIN = yourSIPdomainName.com
```

When you make a call from a Cisco 7940/7960 phone with the local Caller ID Block feature enabled, the called endpoint still displays your number. To work around this issue, use the Calling Number Block FNE in Avaya Communication Manager instead of the local feature in the phone.

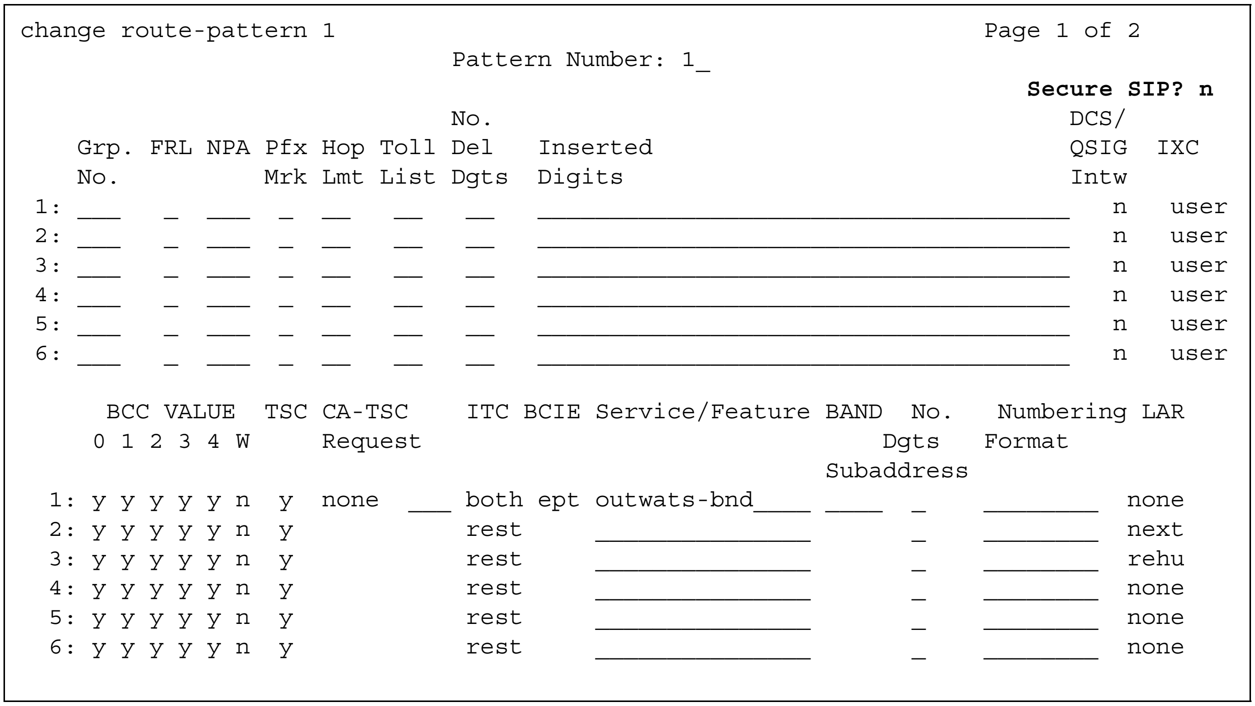
Route Pattern screen

The **Route Pattern** screen defines the route patterns used by Communication Manager. Each route pattern contains a list of trunk groups that can be used to route the call. The maximum number of route patterns and trunk groups depends on the configuration and memory available in your system.

AAR analysis and ARS analysis determine which trunks calls use. You can convert an AAR number into an international number, and insert an area code in an AAR number to convert an on-network number to a public network number. Also, when a call directly accesses a local central office (CO), if the long-distance carrier provided by your CO is not available, then Communication Manager can insert the dial access code for an alternative carrier into the digit string.

The SIP-related fields are in bold on the screen shown in Figure 11. Administering this screen is not required to make SIP work properly.

Figure 11: Route Pattern screen



```
change route-pattern 1                                             Page 1 of 2
                              Pattern Number: 1_
                                                                      Secure SIP? n
                              No.                                        DCS/
    Grp. FRL NPA Pfx Hop Toll Del   Inserted                             QSIG  IXC
    No.          Mrk Lmt List Dgts  Digits                               Intw
 1: ___   _  ___  _  __   __   __    _____________________________________   n   user
 2: ___   _  ___  _  __   __   __    _____________________________________   n   user
 3: ___   _  ___  _  __   __   __    _____________________________________   n   user
 4: ___   _  ___  _  __   __   __    _____________________________________   n   user
 5: ___   _  ___  _  __   __   __    _____________________________________   n   user
 6: ___   _  ___  _  __   __   __    _____________________________________   n   user

      BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature BAND  No.   Numbering LAR
     0 1 2 3 4 W     Request                                Dgts   Format
                                                        Subaddress
  1: y y y y y n  y  none  ___ both ept outwats-bnd____ ____  _    ________  none
  2: y y y y y n  y            rest     _______________       _    ________  next
  3: y y y y y n  y            rest     _______________       _    ________  rehu
  4: y y y y y n  y            rest     _______________       _    ________  none
  5: y y y y y n  y            rest     _______________       _    ________  none
  6: y y y y y n  y            rest     _______________       _    ________  none
```

Secure SIP

You will need to evaluate the setting of the **Secure SIP?** field in the Route Pattern screen when the end-to-end solution supports the SIPS protocol.

The only instance for a **y** in this field is when the source provider *requires* a secure SIP protocol.

In most instances, leave this field set to **n**.

Valid entries	Usage
y/n	Specify whether the SIP: or SIPS: prefix will be used, if the call is routed to a SIP trunk preference. If SIP trunks are not specified as SIP: or SIPS: , the call will be routed over whatever trunk is specified. Therefore, to ensure a SIP TLS connection when such a route-pattern is invoked, only SIP trunks should be specified. Default is **n**.

To administer the Secure SIP field, choose the behavior you want from the following table.

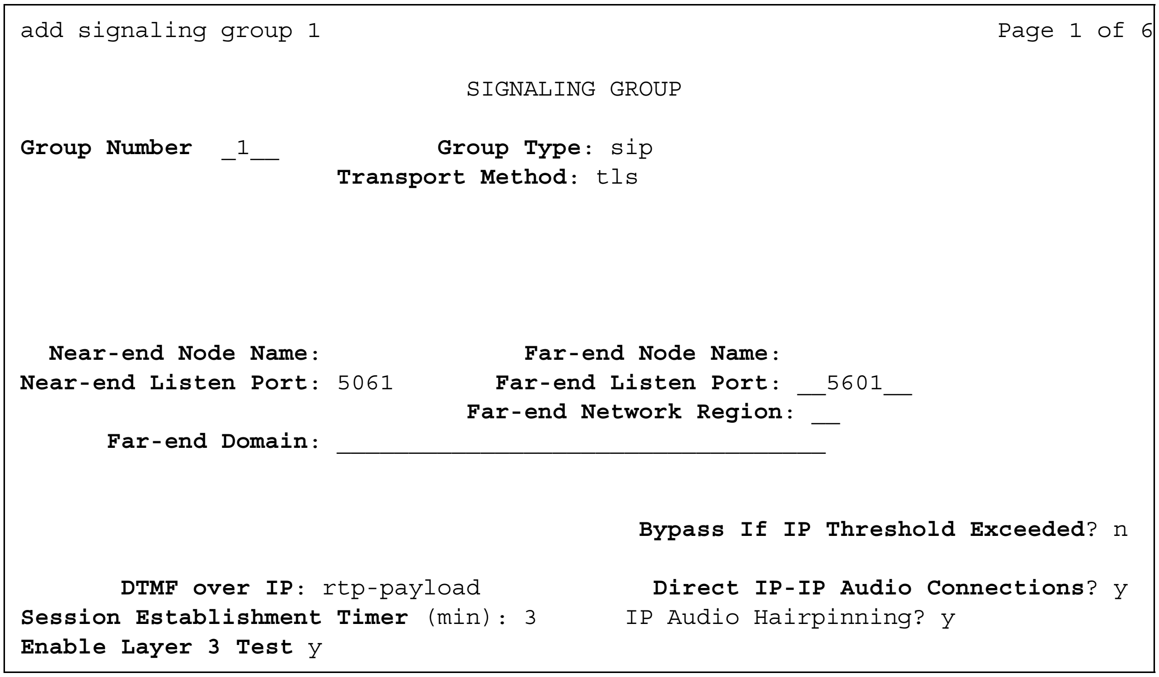
Original Request-URI	Secure SIP?	Final Request-URI
SIP	Y	SIPS
SIPS	N	SIPS
SIP	N	SIP
SIPS	Y	SIPS
NA—non-sip trunk or endpoint	Y	SIPS
NA—non-sip trunk or endpoint	N	SIP

Signaling Group Page 1 screen

The system displays the Signaling Group screen shown in Figure 12 when **sip** is the Group Type field on this page.

Check and administer all fields on this screen. SIP-specific fields are in bold.

Figure 12: Signaling Group screen, Page 1



```
add signaling group 1                                               Page 1 of 6

                               SIGNALING GROUP

Group Number  _1__           Group Type: sip
                      Transport Method: tls




  Near-end Node Name:              Far-end Node Name:
Near-end Listen Port: 5061       Far-end Listen Port: __5601__
                               Far-end Network Region: __
      Far-end Domain: __________________________________


                                           Bypass If IP Threshold Exceeded? n

       DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer (min): 3      IP Audio Hairpinning? y
Enable Layer 3 Test y
```

Group Number

This is a display-only field showing the signaling group, as shown in Figure 12.

Group Type

This field describes the type of protocol to be used with the signaling group. Select **SIP** in this field and the screen changes to show only SIP-applicable fields, as shown in the Signaling Group screen, Page 1.

Valid entries	Usage
sip	Use for SIP on the Avaya S8300, S8500, S8700/S8710 IP-Connect, or S8700/S8710 Multi-Connect media servers only.

Transport Method

The screen in the Signaling Group screen, Page 1 displays this field *only* when the value of the entry in the **Group Type** field is **sip**. Make sure that the default **tls** is selected in this field. No other value is supported.

Valid entries	Usage
tls	Default (secure) transport method is TLS. This is the only method supported.

Near-end Node Name

The screen shown in the Signaling Group screen, Page 1 displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**. Type the node name for the CLANS/procr/PE IP interface in this media server.

Additionally, the node name must be administered on the **IP Node Names** screen and the **IP Interfaces** screen.

Valid entries	Usage
Name of an administered IP node	Uniquely identifies the near-end node.

Far-end Node Name

The screen displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**. Type the node name for the SIP proxy server used for trunks assigned to this signaling group. The node name must be administered on the **IP Node Names** screen. See the Signaling Group screen, Page 1.

Valid entries	Usage
Name of an administered IP node.	Describes the far-end node.

Tip:

If either the node name or port differs for each SIP signaling group, you have different SIP signaling connections, and you should administer a maximum of 10 using TLS. If you administer more than 10 TLS signaling connections, and they are all in use at the same time, the results may be unpredictable. Note that if the node names and ports match, you may administer as many identical SIP signaling groups using TLS as desired.

Near-end Listen Port

The screen displays this field when the **Group Type** field is either **h.323** or **sip**. The **Near-end Listen Port** field defaults to 5061 for SIP over TLS. See the Signaling Group screen, Page 1.

For SIP, set this to 5061.

Valid entries	Usage
1719, **1720**, or **5000** through **5999**	Type an unused port number. The recommended port for SIP over TLS is 5061.

Far-end Listen Port

The screen displays this field when the **Group Type** field is either **h.323** or **sip**. See the Signaling Group screen, Page 1.

For SIP, set this to 5061.

Valid entries	Usage
1 through **65535**	Type the same number as entered in the **Near-end Listen Port** field, that is, port entry 5061 for SIP over TLS.

Far-end Network Region

The screen displays this field when the **Group Type** field is either **h.323** or **sip**. This field shows the number of the network region that is assigned to the far-end of the trunk group. See the Signaling Group screen, Page 1.

Valid entries	Usage
1-250 or blank	Type the network region number that is assigned to the far end of the trunk group. The region number is used to obtain the codec set used for negotiation of trunk bearer capability. Leave blank to select the region of the near-end node by default.

Far-end Domain

The screen displays this field only when the value of the entry in the **Group Type** field is **sip**. See the Signaling Group screen, Page 1.

Valid entries	Usage
Maximum of 40-character string, or blank	Enter the fully qualified domain name or IP address for the destination proxy server. For example, to route SIP calls within your enterprise, enter the domain assigned to your proxy server. For external SIP calling, the domain name could be that of your SIP service provider. If blank, the far-end IP address is used.

Bypass If IP Threshold Exceeded

The screen displays this field when the **Group Type** field is either **h.323** or **sip**. See the Signaling Group screen, Page 1.

Valid entries	Usage
y/n	Type **y** to automatically remove from service the trunks assigned to this signaling group when IP transport performance falls below limits. These limits are set on the **Maintenance-Related System Parameters** screen.

DTMF over IP

The screen displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**. See the Signaling Group screen, Page 1.

For SIP, this must be set at the default value of **rtp-payload**.

Valid entries	Usage
rtp-payload	SIP trunks require **rtp-payload**.

Session Establishment Timer

This field determines how long the system waits before tearing down a ring no answer call. The default is 3 minutes. See the Signaling Group screen, Page 1.

For SIP, the recommendation is to set this to 3 minutes.

Valid entries	Usage
3 through **120**	The time in minutes Communication Manager waits before tearing down a ring no answer call.

Direct IP-IP Audio Connections

The screen displays this field when the value of the entry in the **Group Type** field is either **h.323** or **sip**. For SIP trunk groups, this is the value that allows direct audio connections between SIP endpoints. See the Signaling Group screen, Page 1.

For SIP, leave this at the default of y. This value must match the setting for the **IP Audio Hairpinning** field.

Valid entries	Usage
y/n	Type **y** to save bandwidth resources and improve sound quality of VoIP transmissions for H.323 or SIP trunk groups.

IP Audio Hairpinning

The screen displays this field when the Group Type field is either h.323 or sip. The IP Audio Hairpinning field entry allows the option for H.323 and SIP-enabled endpoints to be connected through the IP circuit pack in the media server or switch, without going through the time division multiplexing (TDM) bus. See the Signaling Group screen, Page 1.

For SIP, leave this at the default of y. This value must match the setting for the **Direct IP-IP Audio Connections** field.

Valid entries	Usage
y/n	Type **y** to enable hairpinning for H.323 or SIP trunk groups. Default is **y**.

Enable Layer 3 Test

Set this field to **y** for SIP.

When the signaling group **Enable Layer 3** Test field is set to **y** for a SIP signaling group, the maintenance test invokes a "transmitting the OPTIONS" request. The ping test becomes disabled.

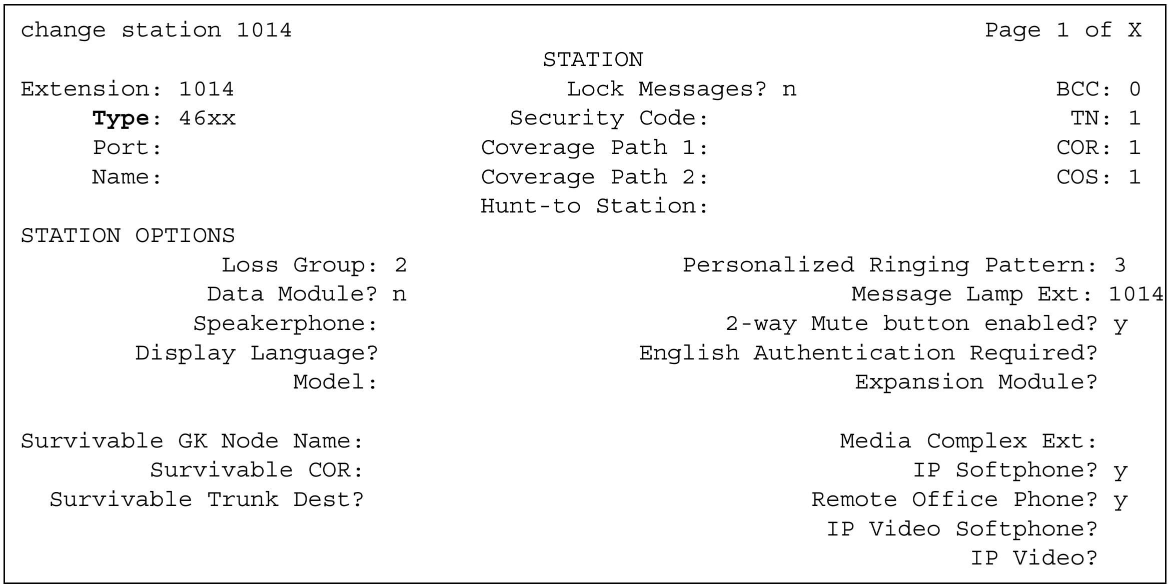
Note that if the field is set to **n** the test shall invoke the existing ping test, and the OPTIONS test shall be disabled.

When the signaling group "Enable Layer 3 Test" field is set to "y" for a SIP signaling group and the test fails, the status trunk/trunk-group command for SIP trunks using that signaling group is reported as being in bypass mode. This way, SIP trunk status reports show trunks that are out of service. See the Signaling Group screen, Page 1.

Station screen, page 1

This screen is not SIP-specific, it must be administered for all installations and so is part of SIP administration. Please check the fields in bold.

Figure 13: Station screen page 1



```
change station 1014                                                Page 1 of X
                                    STATION
Extension: 1014                       Lock Messages? n                  BCC: 0
     Type: 46xx                   Security Code:                         TN: 1
     Port:                      Coverage Path 1:                        COR: 1
     Name:                      Coverage Path 2:                        COS: 1
                                Hunt-to Station:
STATION OPTIONS
              Loss Group: 2                   Personalized Ringing Pattern: 3
             Data Module? n                               Message Lamp Ext: 1014
            Speakerphone:                        2-way Mute button enabled? y
        Display Language?                 English Authentication Required?
                   Model:                                 Expansion Module?

Survivable GK Node Name:                                 Media Complex Ext:
         Survivable COR:                                      IP Softphone? y
  Survivable Trunk Dest?                               Remote Office Phone? y
                                                        IP Video Softphone?
                                                                  IP Video?
```

Type

Set the type of station to **DCP** for 6424 endpoints or **IP** for 4600 series endpoints.

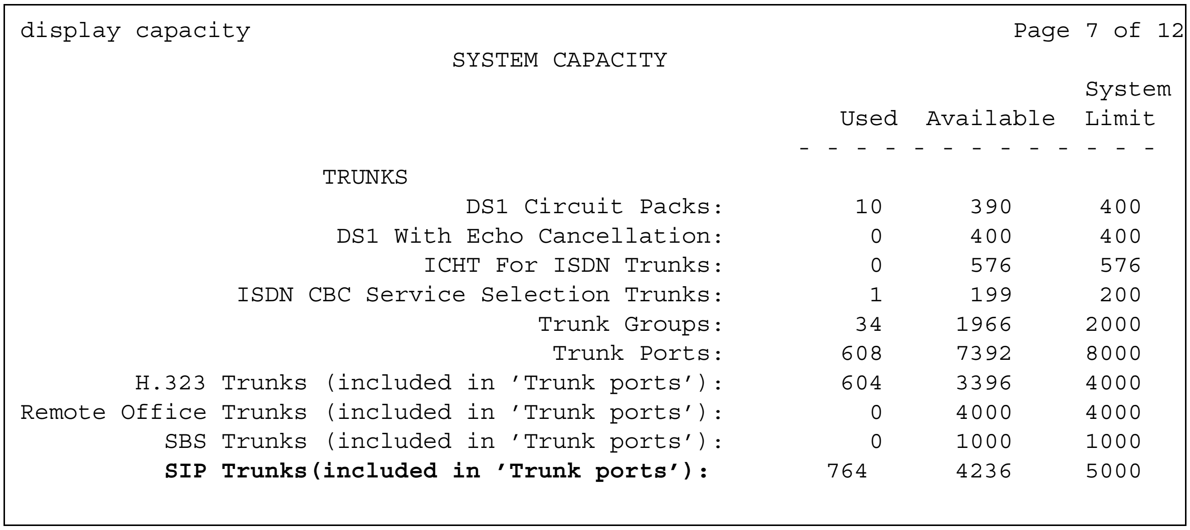
If using 46xx as the Type, you will have minor alarm for these stations. You may ignore these alarms.

If you set the Type to DCP, there are some undesirable interactions with the TTI as well as other features.

System Capacity screen

The SIP-related fields are in bold on this screen, as shown in Figure 14:

Figure 14: System Capacity screen



```
display capacity                                                     Page 7 of 12
                              SYSTEM CAPACITY
                                                                          System
                                                         Used  Available  Limit
                                                      - - - - - - - - - - - - -
                     TRUNKS
                               DS1 Circuit Packs:         10      390      400
                      DS1 With Echo Cancellation:          0      400      400
                            ICHT For ISDN Trunks:          0      576      576
               ISDN CBC Service Selection Trunks:          1      199      200
                                    Trunk Groups:         34     1966     2000
                                     Trunk Ports:        608     7392     8000
        H.323 Trunks (included in ’Trunk ports’):        604     3396     4000
Remote Office Trunks (included in ’Trunk ports’):          0     4000     4000
          SBS Trunks (included in ’Trunk ports’):          0     1000     1000
          SIP Trunks(included in ’Trunk ports’):        764      4236     5000
```

Note that system trunking capacity varies, based on the media server. See the document *Capacities Table* for more information. The capacities table document is for Avaya use only and not available to customers. Customers should consult their Avaya representative.

SIP Trunks

This field shows the number of administered, in use, and available SIP trunks.

System-Parameters screens

This section describes each page of the various System Parameters screens. Valid data entry for each screen follows the screen example.

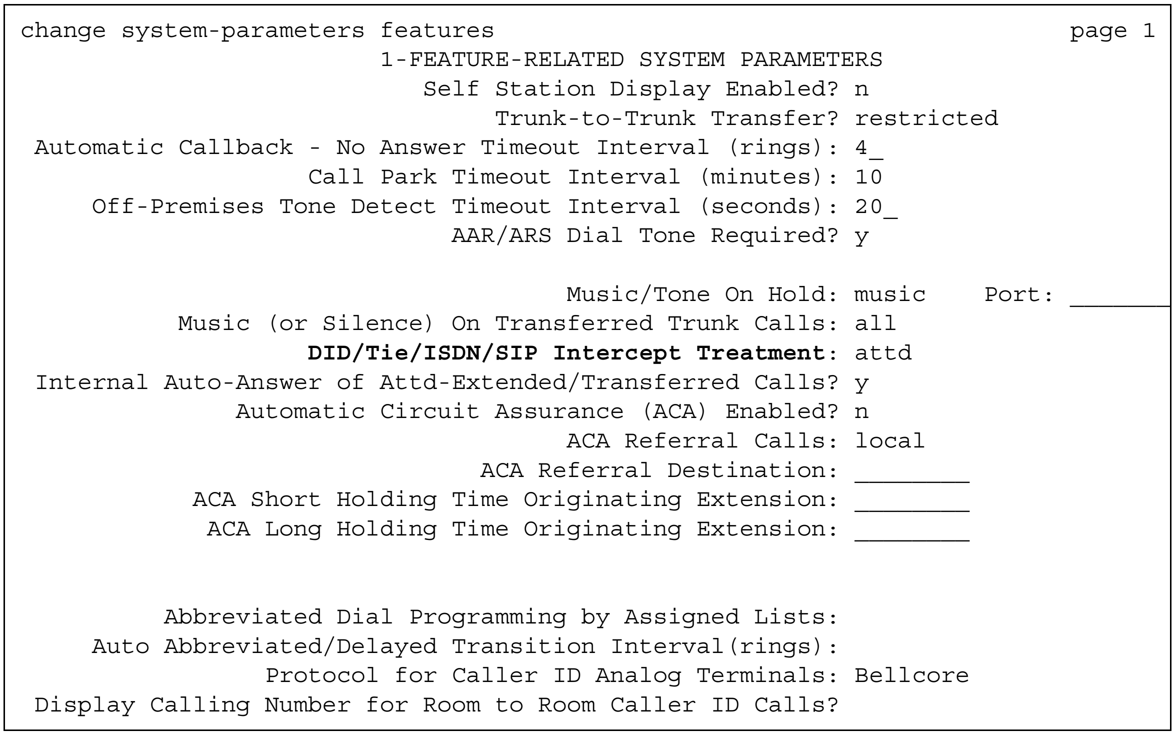
- System Parameters Features screen, page 1 on page 75
- System Parameters Call Coverage/Call Forwarding screen, page 2 on page 77
- System-Parameters Customer-Options screen, page 1 on page 78
- System Parameters Customer Options screen, page 2 on page 80
- System Parameters Customer Options screen, page 4 on page 81
- System Parameters Customer Options screen, page 5 on page 82

System Parameters Features screen, page 1

The Feature-Related System Parameters screen in Figure 15 shows the SIP-related information in bold.

Administer other fields as necessary for your system.

Figure 15: System Parameters Feature screen Page 1



```
change system-parameters features                                        page 1
                         1-FEATURE-RELATED SYSTEM PARAMETERS
                            Self Station Display Enabled? n
                                 Trunk-to-Trunk Transfer? restricted
 Automatic Callback - No Answer Timeout Interval (rings): 4_
                    Call Park Timeout Interval (minutes): 10
     Off-Premises Tone Detect Timeout Interval (seconds): 20_
                              AAR/ARS Dial Tone Required? y

                                      Music/Tone On Hold: music    Port: ________
           Music (or Silence) On Transferred Trunk Calls: all
                    DID/Tie/ISDN/SIP Intercept Treatment: attd
 Internal Auto-Answer of Attd-Extended/Transferred Calls? y
               Automatic Circuit Assurance (ACA) Enabled? n
                                      ACA Referral Calls: local
                                ACA Referral Destination: ________
            ACA Short Holding Time Originating Extension: ________
             ACA Long Holding Time Originating Extension: ________


          Abbreviated Dial Programming by Assigned Lists:
     Auto Abbreviated/Delayed Transition Interval(rings):
                 Protocol for Caller ID Analog Terminals: Bellcore
 Display Calling Number for Room to Room Caller ID Calls?
```

DID/Tie/ISDN/SIP Intercept Treatment

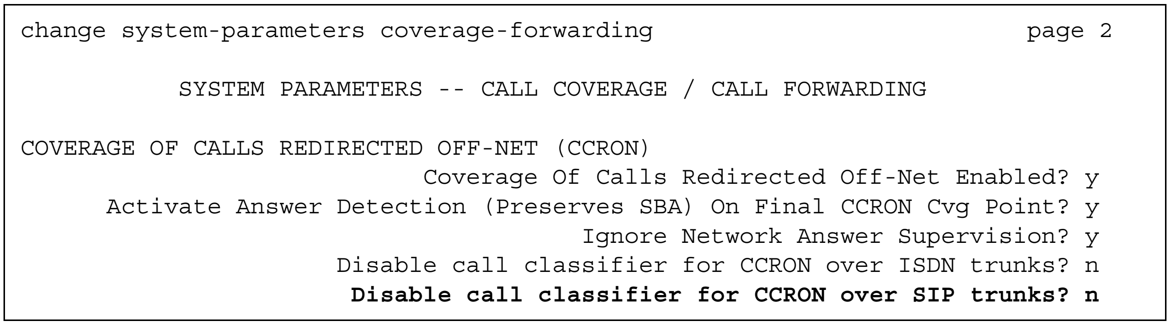
There is only one field in Figure 15 that must be administered for SIP. Set this field to **attd**.

Valid entries	Usage
Extension of a recorded announcement	Toll charges do not apply to DID and private network calls routed to an announcement. **NOTE:** If entering a Multi-Location Dial Plan shortened extension, note the following: When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application when assigning shortened extensions.
attd	For system security, Avaya recommends entering **attd** in this field. This routes intercept calls to the attendant and, if the attendant receives several of these, indicates a problem.

System Parameters Call Coverage/Call Forwarding screen, page 2

The SIP-related fields are in bold on Figure 16.

Figure 16: System Parameters—Call Coverage/Call Forwarding screen



```
change system-parameters coverage-forwarding                                 page 2

           SYSTEM PARAMETERS -- CALL COVERAGE / CALL FORWARDING

COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)
                            Coverage Of Calls Redirected Off-Net Enabled? y
      Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point? y
                                       Ignore Network Answer Supervision? y
                      Disable call classifier for CCRON over ISDN trunks? n
                       Disable call classifier for CCRON over SIP trunks? n
```

For more details on the other fields on this screen, see the *Avaya Communication Manager Administrator Guide*, 03-300509.

Disable call classifier for CCRON over SIP trunks

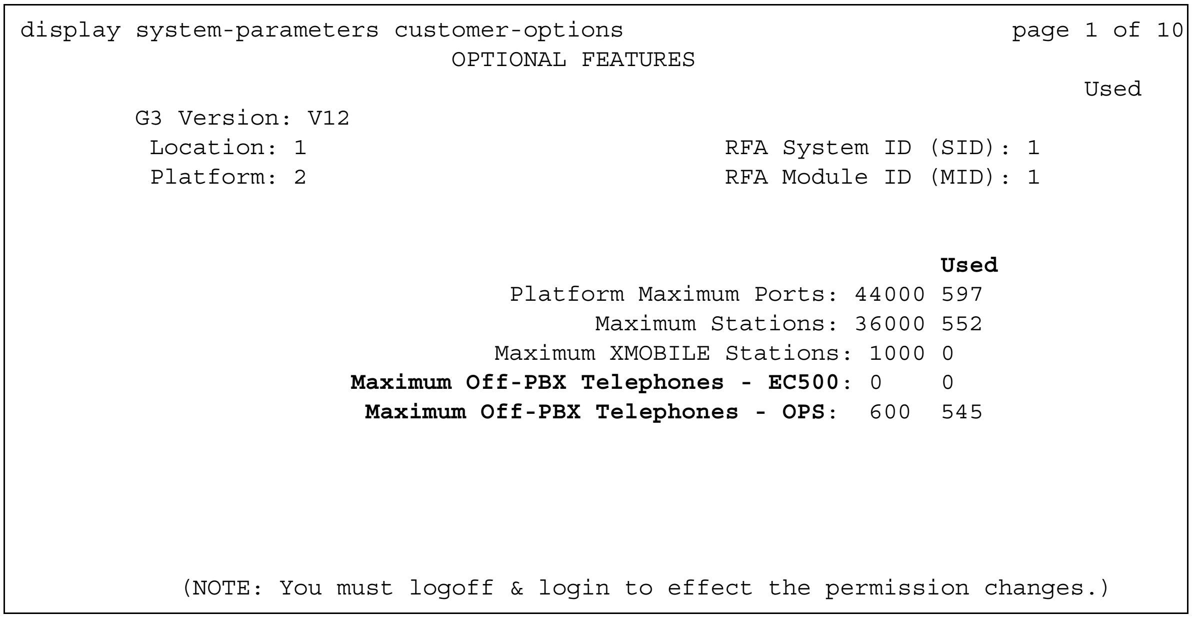
This field Figure 16 directs Communication Manager to dispense with the call classifier on interworked calls and rely on the SIP trunk signalling messages. For SIP, set this field to **n**.

Valid entries	Usage
y	Use **y** to disable the call classifier for CCRON calls over interworked trunk facilities.
n	Use **n** to enable the call classifier for CCRON calls over interworked trunk facilities.

System-Parameters Customer-Options screen, page 1

Administer or check all fields on the screen shown in Figure 17 to meet the needs of your system.

Figure 17: System Parameters Customer Options screen, page 1



```
display system-parameters customer-options                           page 1 of 10
                              OPTIONAL FEATURES
                                                                          Used
        G3 Version: V12
         Location: 1                            RFA System ID (SID): 1
         Platform: 2                            RFA Module ID (MID): 1


                                                                Used
                                  Platform Maximum Ports: 44000 597
                                        Maximum Stations: 36000 552
                                 Maximum XMOBILE Stations: 1000 0
                       Maximum Off-PBX Telephones - EC500: 0    0
                        Maximum Off-PBX Telephones - OPS:  600  545





            (NOTE: You must logoff & login to effect the permission changes.)
```

The Avaya license file controls the fields on this screen. The web-based RFA process generates these license files for customers.

The customer views this screen to see how many and what type of off-PBX phones the license supports. Normally, this screen is read only.

However, an administrator with init login privileges can type in values that represent a portion of the licensed values.

Depending on your login privileges, you can view or edit the fields shown.

Maximum Off-PBX Telephones - EC500

Licensing obtained for this feature applies to EC500 and CSP phones. See Figure 17.

Maximum Off-PBX Telephones - OPS

Licensing for this feature applies to OPS phones, which are SIP phones supporting advanced SIP telephony. See Figure 17.

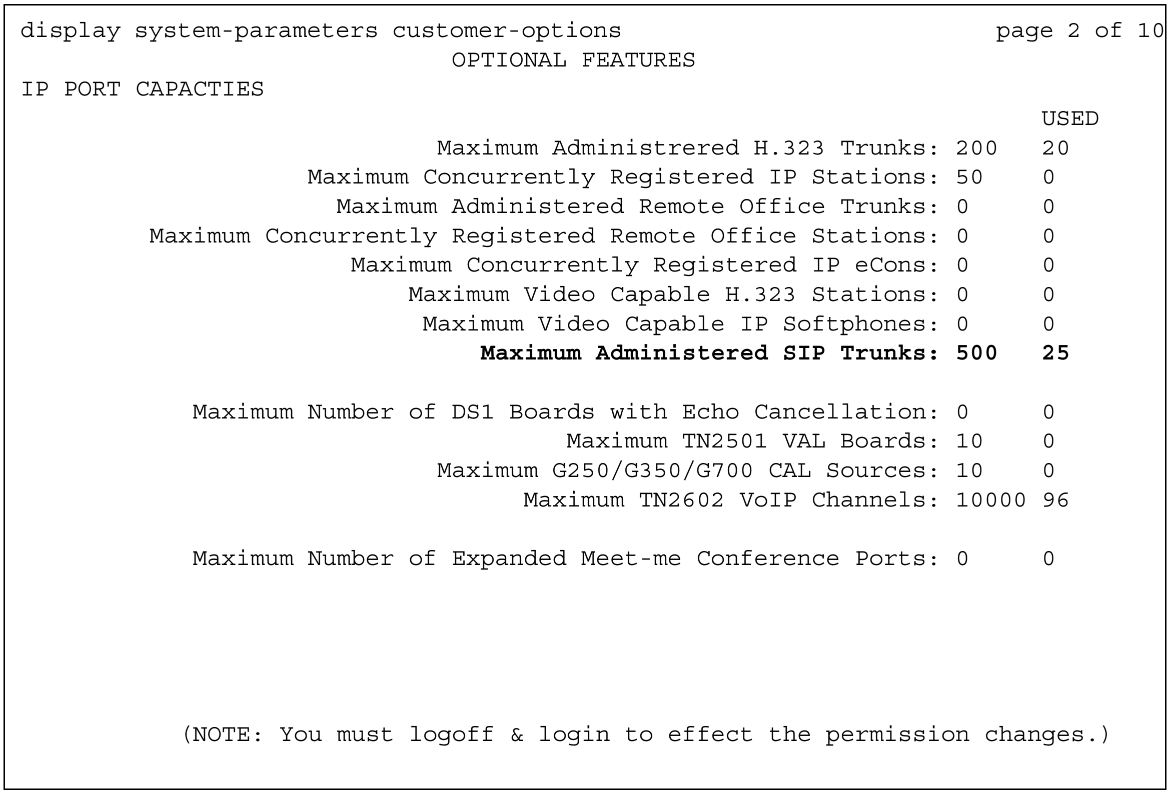
Used

This column in the System Parameters Customer Options screen, page 1 shows the actual current usage as compared to the system maximum for each field. The Used column is always display only, and indicates the number of the applications that are administered on the Off-PBX Station Mapping screen page 1 on page 58.

System Parameters Customer Options screen, page 2

The SIP-related fields are in bold in this screen.

Figure 18: System Parameters Customer Options screen, page 2



```
display system-parameters customer-options                          page 2 of 10
                              OPTIONAL FEATURES
IP PORT CAPACTIES
                                                                       USED
                             Maximum Administrered H.323 Trunks: 200   20
                    Maximum Concurrently Registered IP Stations: 50    0
                      Maximum Administered Remote Office Trunks: 0     0
         Maximum Concurrently Registered Remote Office Stations: 0     0
                       Maximum Concurrently Registered IP eCons: 0     0
                           Maximum Video Capable H.323 Stations: 0     0
                            Maximum Video Capable IP Softphones: 0     0
                                Maximum Administered SIP Trunks: 500   25

            Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                                      Maximum TN2501 VAL Boards: 10    0
                             Maximum G250/G350/G700 CAL Sources: 10    0
                                   Maximum TN2602 VoIP Channels: 10000 96

            Maximum Number of Expanded Meet-me Conference Ports: 0     0




           (NOTE: You must logoff & login to effect the permission changes.)
```

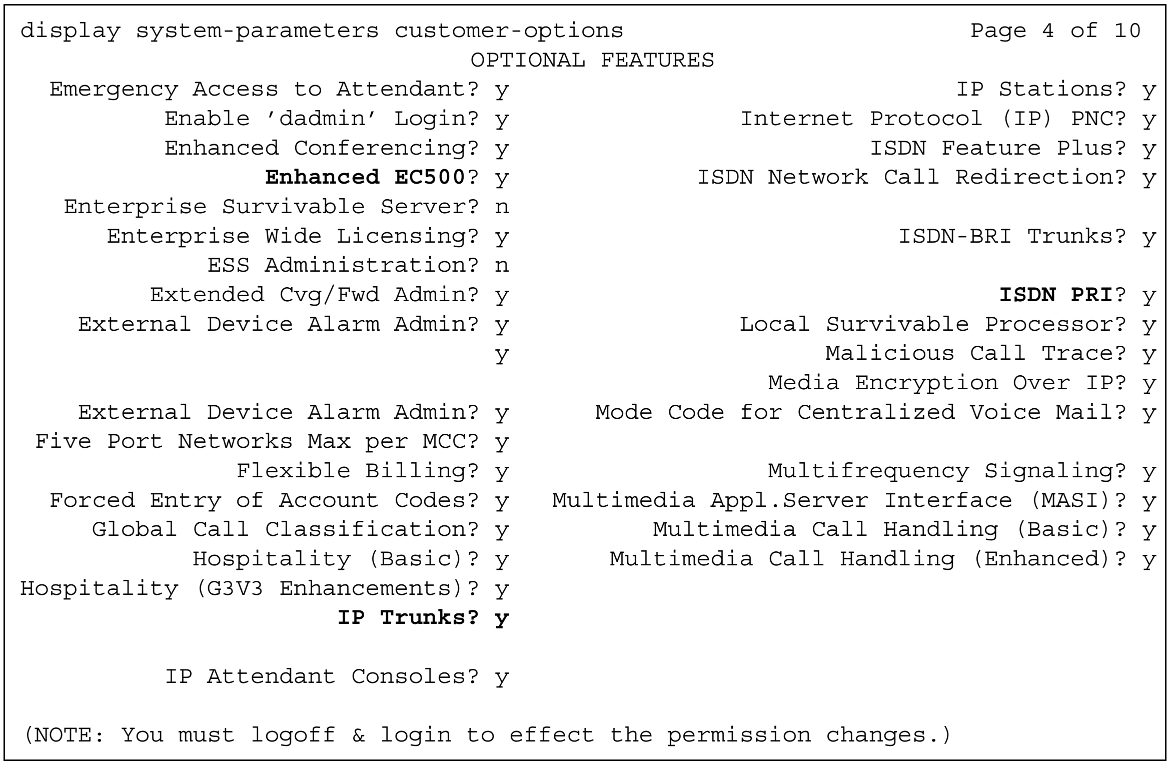
Maximum Administered SIP Trunks

This field in Figure 18 limits the number of SIP trunks administered.

System Parameters Customer Options screen, page 4

The SIP-related fields on this screen are in bold.

Figure 19: System Parameters Customer Options screen, page 4



```
display system-parameters customer-options                        Page 4 of 10
                               OPTIONAL FEATURES
  Emergency Access to Attendant? y                               IP Stations? y
          Enable ’dadmin’ Login? y                Internet Protocol (IP) PNC? y
          Enhanced Conferencing? y                        ISDN Feature Plus? y
                 Enhanced EC500? y             ISDN Network Call Redirection? y
   Enterprise Survivable Server? n
      Enterprise Wide Licensing? y                           ISDN-BRI Trunks? y
             ESS Administration? n
         Extended Cvg/Fwd Admin? y                                  ISDN PRI? y
    External Device Alarm Admin? y                Local Survivable Processor? y
                                 y                      Malicious Call Trace? y
                                                    Media Encryption Over IP? y
    External Device Alarm Admin? y      Mode Code for Centralized Voice Mail? y
 Five Port Networks Max per MCC? y
               Flexible Billing? y                  Multifrequency Signaling? y
  Forced Entry of Account Codes? y   Multimedia Appl.Server Interface (MASI)? y
     Global Call Classification? y          Multimedia Call Handling (Basic)? y
            Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? y
                      IP Trunks? y

          IP Attendant Consoles? y

(NOTE: You must logoff & login to effect the permission changes.)
```

ISDN PRI

Provides Integrated Services Digital Network (ISDN-PRI) software for either a switching-hardware platform migration only or a switching-hardware platform migration in combination with a software release upgrade. Also provides signaling support for H.323 signaling. Set to **y** for SIP. See Figure 19 above.

Enhanced EC500

As shown in Figure 19, set this to **y**. This setting provides mobile call services including "Anytime Anywhere" accessibility with One Number availability and Origination mapping.

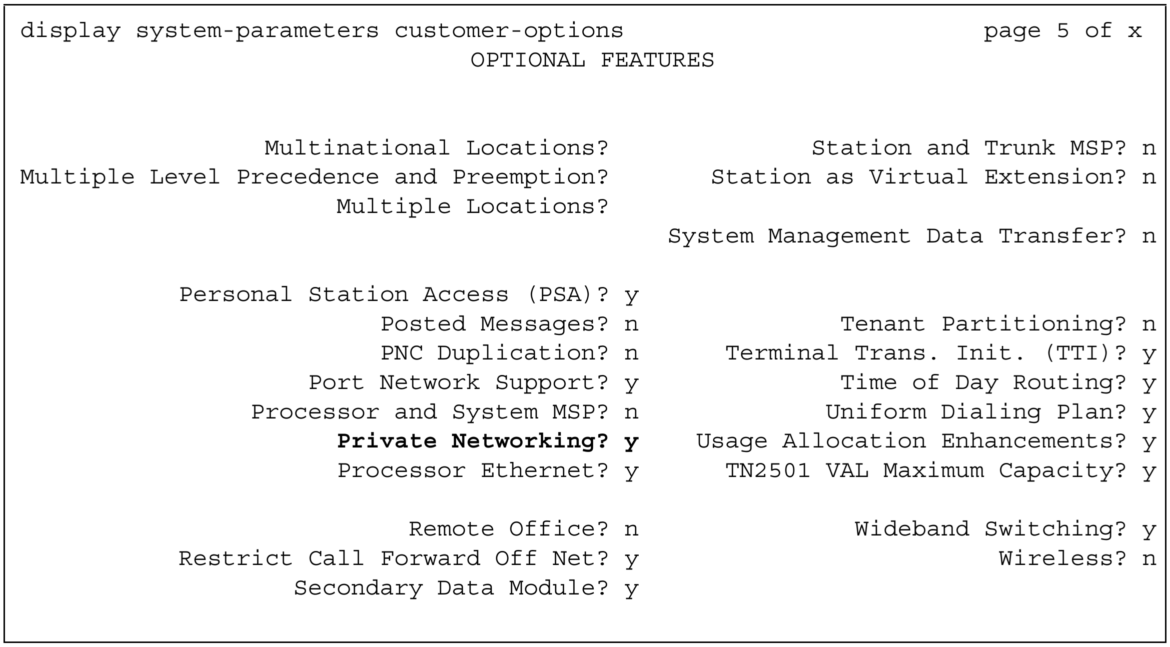
IP Trunks

Controls permission to administer H.323 trunks. Must be **y** for IP trunks. See Figure 19: System Parameters Customer Options screen, page 4.

System Parameters Customer Options screen, page 5

The SIP-related fields on this screen are in bold.

Figure 20: System Parameters Customer Options screen, page 5



```
display system-parameters customer-options                         page 5 of x
                               OPTIONAL FEATURES


                 Multinational Locations?              Station and Trunk MSP? n
Multiple Level Precedence and Preemption?       Station as Virtual Extension? n
                      Multiple Locations?
                                             System Management Data Transfer? n

           Personal Station Access (PSA)? y
                         Posted Messages? n              Tenant Partitioning? n
                         PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                    Port Network Support? y              Time of Day Routing? y
                Processor and System MSP? n             Uniform Dialing Plan? y
                      Private Networking? y     Usage Allocation Enhancements? y
                      Processor Ethernet? y       TN2501 VAL Maximum Capacity? y

                           Remote Office? n               Wideband Switching? y
           Restrict Call Forward Off Net? y                         Wireless? n
                   Secondary Data Module? y
```

Private Networking

Upgrades PNA or ETN software RTU purchased with earlier systems. Set this to y if you want to enable AAR access codes or ARS access codes 1 and 2 on the Feature Access Codes screen.

Trunk Group screens

This section describes each page of the Trunk Group screens. Valid data entry for each screen follows the screen example.

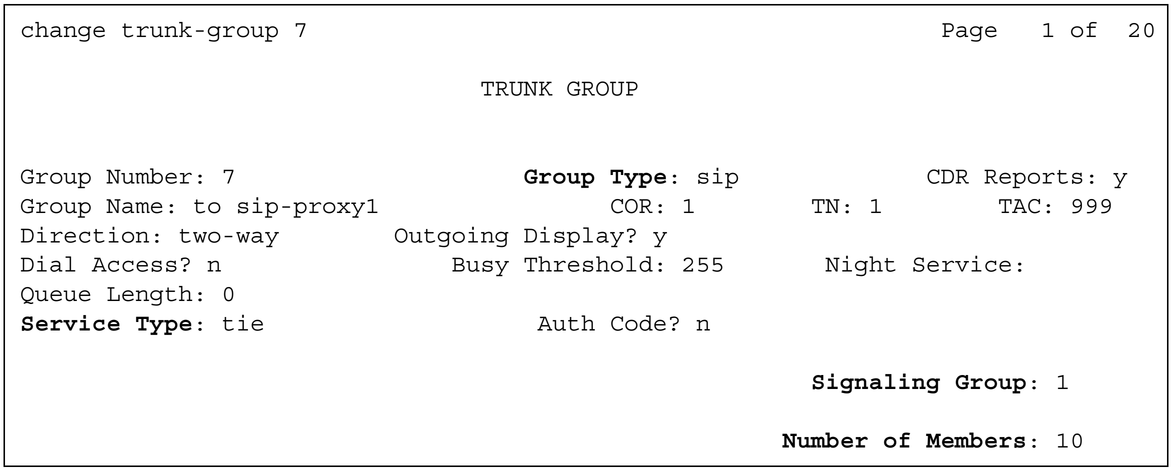
- Trunk Group screen, Page 1 on page 83
- Trunk Group screen, Page 2 on page 91
- Trunk Group screen, Page 3 on page 93

Trunk Group screen, Page 1

The system displays the **Trunk Group** screen shown in Figure 21, when **sip** is the **Group Type** on page 1.

Check or administer all the values on this screen. SIP-specific fields are in bold.

Figure 21: Trunk Group screen, page 1



```
change trunk-group 7                                            Page   1 of  20

                                TRUNK GROUP


Group Number: 7                    Group Type: sip             CDR Reports: y
Group Name: to sip-proxy1                COR: 1        TN: 1        TAC: 999
Direction: two-way        Outgoing Display? y
Dial Access? n                Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 1

                                                     Number of Members: 10
```

Group Number

In the Trunk Group screen, page 1, this field contains the group number assigned to this group when the trunk group was added.

Group Type

In the Trunk Group screen, page 1, type **sip** to specify the trunk group as SIP.

Tip:

Busy-out the trunk group before you change the group type. Release the trunk group after you make the change. For more information about busying out and releasing trunk groups, see your system's maintenance documentation.

Valid entries	Usage
sip	Use SIP trunks to connect a media server running Communication Manager to a SIP proxy home server.

CDR Reports

In the Trunk Group screen, page 1, set this field according to the kind of call detail records (CDR) you want to generate.

Valid entries	Usage
y	All outgoing calls on this trunk group generate call detail records. To generate CDRs on incoming trunks, type **n** in the **Record Outgoing Calls Only** field on the **CDR System Parameters** screen.
n	Calls over this trunk group will not generate call detail records.
r (ring-intvl)	Generate CDR records for both incoming and outgoing calls. In addition, the following ringing interval CDR records are generated: ● Abandoned calls: The system creates a record with a condition code of **H**, indicating the time until the call was abandoned. ● Answered calls: The system creates a record with a condition code of **G**, indicating the interval from start of ring to answer. ● Calls to busy stations: The system creates a record with a condition code of **I** indicating a recorded interval of 0.

Group Name

On Trunk Group screen, page 1, set this field to uniquely identify a trunk group.

Valid entries	Usage
1 to **27** characters	Enter a unique name that provides information about the trunk group. Do not use the default entry or the group type (DID, WATS) here. For example, you might use names that identify the vendor and function of the trunk group: USWest Local, Sprint Toll, Level(3) SIP.

COR

In Trunk Group screen, page 1, the setting for this field depends on your system.

Decisions regarding the use of Class of Restriction (COR) and Facility Restriction Levels (FRLs) should be made with an understanding of their implications for allowing or denying calls when AAR/ARS/WCR route patterns are accessed. See Chapter 5 of the *Avaya Toll Fraud and Security Handbook*, doc ID 555-025-600, for details on using COR and FRLs.

Valid entries	Usage
0 to **95**	Enter a class of restriction (COR). Classes of restriction control access to trunk groups, including trunk-to-trunk transfers.

Tip:

Remember that facility restriction levels are assigned to *classes* of restriction. Even if two trunk groups have classes of restriction that allow a connection, different facility restriction levels may prevent operations such as off-net call forwarding or outgoing calls by remote access users.

TN

On Trunk Group screen, page 1, set this field to assign a trunk to a partition.

In the Customer Options screen, if Tenant Partitioning is set to **n**, this field is present on the Trunk Screen but does not function. Go the Customer Options screen if you suspect incorrect operation.

Valid entries	Usage
1 to **100**	Type a tenant partition number to assign this trunk group to the partition. Enter the digit 1 in this field to assign the trunk to the universal group which can be called by any other TN group.

Tip:

Double-check your entry. If you accidentally type an unassigned tenant partition number, the system accepts the entry but no calls go to the trunk group.

TAC

Type the trunk access code (TAC) for each trunk group. Assign a different TAC to each trunk group. CDR reports use the TAC to identify each trunk group. Each trunk must have a different TAC. This field is on Trunk Group screen, page 1.

Valid entries	Usage
1- to 4-digit number	Type any number that fits the format for trunk access codes or dial access codes defined in your dial plan. NOTE: Although this field is required, trunk groups of type SIP cannot be dialed by using TAC. The TAC you type here only identifies them on CDR reports.
asterisk (*) and pound sign (#)	* and # may be used as the first character in a TAC.

Direction

On Trunk Group screen, page 1, enter the direction of the traffic on this trunk group. The entry in this field affects which timers appear on the Administrable Timers page. The system displays this field for all trunk groups except DID and CPE.

Valid entries	Usage
incoming	
outgoing	
two-way	Enter **two-way** for Network Call Redirection.

Outgoing Display

In Trunk Group screen, page 1, this field allows display telephones to show the name and number of the trunk group used for an outgoing call before the call is connected. This information may be useful to you when you are trying to diagnose trunking problems.

Valid entries	Usage
y	Displays the trunk group name and number.
n	Displays the digits the caller dials.

Dial Access

In Trunk Group screen, page 1, this field controls whether users can route outgoing calls through an outgoing or two-way trunk group by dialing its trunk access code. Allowing dial access does not interfere with the operation of AAR/ARS. Dial access to SIP trunks is not allowed.

Valid entries	Usage
n	The entry **n** is used for SIP trunks, no others. Prevents users from accessing the trunk group by dialing its access code. Attendants can still select this trunk group with a Trunk Group Select button. This is the default entry.

Busy Threshold

In Trunk Group screen, page 1, this field specifies the threshold limit for the number of trunks that could be simultaneously active. Once the threshold is reached, any additional calls that *would* result in accessing that trunk group get redirected to the attendant. The attendant takes control of that trunk group and the access to the trunk members.

Use this field if you want attendants to control access to outgoing and two-way trunk groups during periods of high use. When the threshold is reached and the warning lamp for that trunk group lights, the attendant can activate trunk group control: internal callers who dial out using a trunk access code will be connected to the attendant, and the attendant can prioritize outgoing calls for the last remaining trunks. Calls handled by AAR and ARS route patterns go out normally.

Valid entries	Usage
0 to **255**	Type the number of trunks that must be busy in order to light the warning lamp on the Attendant Console. For example, if there are 30 trunks in the group and you want to alert the attendant whenever 25 or more are in use, type **25**.

The S8700/S8710 supports a maximum of 30000 busy hour call completions (BHCC).

The S8300 remains at a maximum of 3600 BHCC.

Night Service

In Trunk Group screen, page 1, this field sets the destination for incoming calls when Night Service is in operation. If a **Night** field on the **Group Member Assignments** page is administered with a different destination, that entry overrides the group destination for that trunk. CPE, DID, and DIOD trunk groups do not support night service.

Tip:

Whenever possible, use a night service destination on your switch to prevent incorrect behavior of some features, even on a DCS network.

Valid entries	Usage
blank	Leave this field blank if the **Trunk Type (in/out)** field is not **auto**.
An extension number (can be a VDN)	Type the extension of your night service destination.
attd	Calls go to the attendant and are recorded as Listed Directory Number (LDN) calls on call detail records.

Queue Length

In Trunk Group screen, page 1, outgoing calls can wait in a queue, in the order in which they were made, when all trunks in a trunk group are busy. If you type **0** in this field, callers receive a busy signal when no trunks are available. If you type a higher number, a caller hears a confirmation tone when no trunk is available for the outgoing call. The caller can then hang up and wait. When a trunk becomes available, Communication Manager calls the extension that placed the original call. The caller hears three short, quick rings. The caller does not need to do anything but pick up the handset and wait. Communication Manager remembers the number the caller dialed and automatically completes the call.

The screen displays this field when the **Direction** field on the screen is set to **outgoing** or **two-way**.

Valid entries	Usage
0	Type **0** for DCS trunks.
1 through **100**	Type the number of outgoing calls that you want to be held waiting when all trunks are busy.

Service Type

In Trunk Group screen, page 1, the **Service Type** field indicates the service to which this trunk group is dedicated. A listing of predefined entries is shown below. In addition to the Services/Features listed in this table, any user-defined Facility Type of **0** (feature) or **1** (service) on the **Network Facilities** screen is allowed. For SIP trunks, only **public-ntwrk** and **tie** are valid.

Valid entries	Usage
public-ntwrk	Public network calls. It is the equivalent of CO (outgoing), DID, or DIOD trunk groups. If **Service Type** is **public-ntwrk** and the trunk is not a SIP trunk, then **Dial Access** can be set to **y**.
tie	Tie trunks. General purpose. This setting is used for systems inside the Avaya network, not for customers.

Auth Code

In Trunk Group screen, page 1, this field affects the level of security for incoming and outgoing calls on the Communication Manager server. The system displays this field if the **Direction** field is **incoming** or **two-way**. The **Auth Code** field can only be **y** if the **Authorization Codes** field is **y** on the System Parameters Feature screen Page 1 ***on page 76***.

Valid entries	Usage
y or **n**	Type **y** to require callers to enter an authorization code in order to tandem a call through an AAR or ARS route pattern. The code will be required even if the facility restriction level of the incoming trunk group is normally sufficient to send the call out over the route pattern.

Signaling Group

In Trunk Group screen, page 1, the screen displays this field only when the value of the entry in the **Group Type** field is **sip**.

The value here must be set as in the previous signaling group screen, in this example, 1.

Valid entries	Usage
1 through **650**	Type the number of the SIP signaling group associated with this trunk group on the Signaling Group Page 1 screen on page 67, **Group Number** field.

This field restricts calling, and requires a code for users below the FRL level for incoming and outgoing calls.

Number of Members

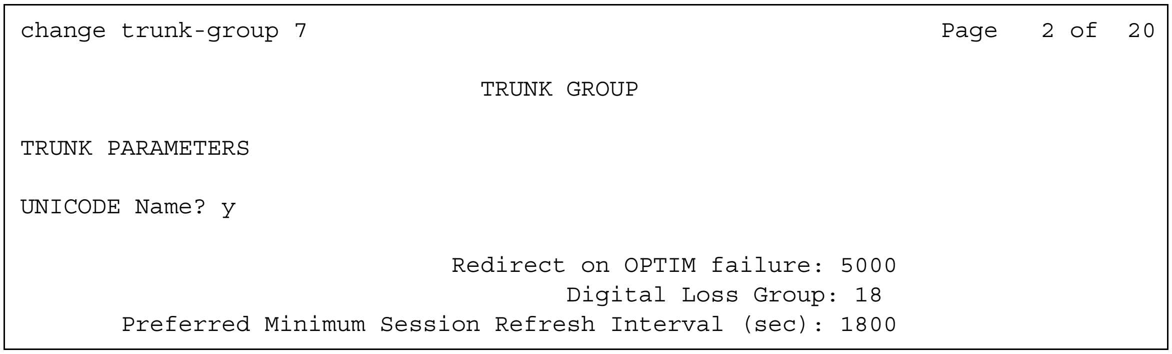
In Trunk Group screen, page 1, the value here must be less than or equal to the maximum administered number for SIP trunks on the System Parameters Custom Options screen. The screen displays this field only when the value of the entry in the **Group Type** field is **sip**.

Valid entries	Usage
1 through **255**	Type the number of SIP trunks that are members of the trunk group. All members of a SIP trunk group will have the same characteristics. NOTE: Member pages for SIP trunk groups are completed automatically based on this entry and are not individually administrable.

Trunk Group screen, Page 2

The SIP-related fields are in bold in this screen.

Figure 22: Trunk Group screen, page 2



```
change trunk-group 7                                            Page   2 of  20

                                TRUNK GROUP

TRUNK PARAMETERS

UNICODE Name? y

                              Redirect on OPTIM failure: 5000
                                      Digital Loss Group: 18
       Preferred Minimum Session Refresh Interval (sec): 1800
```

UNICODE Name

In Trunk Group screen, page 2 this field determines which table of names to use to display the name, the legacy or the UTF-8 character table.

Valid entries	Usage
y or **n**	Type **n** to use the table with legacy names. Type **y** to use the table with UTF-8 format if your system might contain Asian language names. Note that fifteen UTF-8 characters can take up to 45 bytes. Also, legacy names support Roman, Cyrillic, Ukrainian, and Katakana characters.

Redirect on OPTIM failure

In Trunk Group screen, page 2, this field is a timer that determines how long to wait for OPTIM to intercede before the call is redirected. Redirect on OPTIM failure is sometimes known as ROOF.

Valid entries	Usage
250 to **32000 milliseconds**	See EC500 documents for the SIP-related uses of OPTIM, that is, OPS.

Digital Loss Group

In Trunk Group screen, page 2, this field determines which administered 2-party row in the loss plan applies to this trunk group if the call is carried over a digital signaling port in the trunk group.

Valid entries	Usage
1 to **19**	Shows the index into the loss plan and tone plan.

Preferred Minimum Session Refresh Interval (sec)

This field on Trunk Group screen, page 2 sets the session refresh timer value of a SIP session. The timer starts when a SIP session is established. Avaya Communication Manager then sends a session refresh request as a Re-INVITE or UPDATE after every timer interval. In this way, an ongoing session is maintained.

For SIP, set this to 1800.

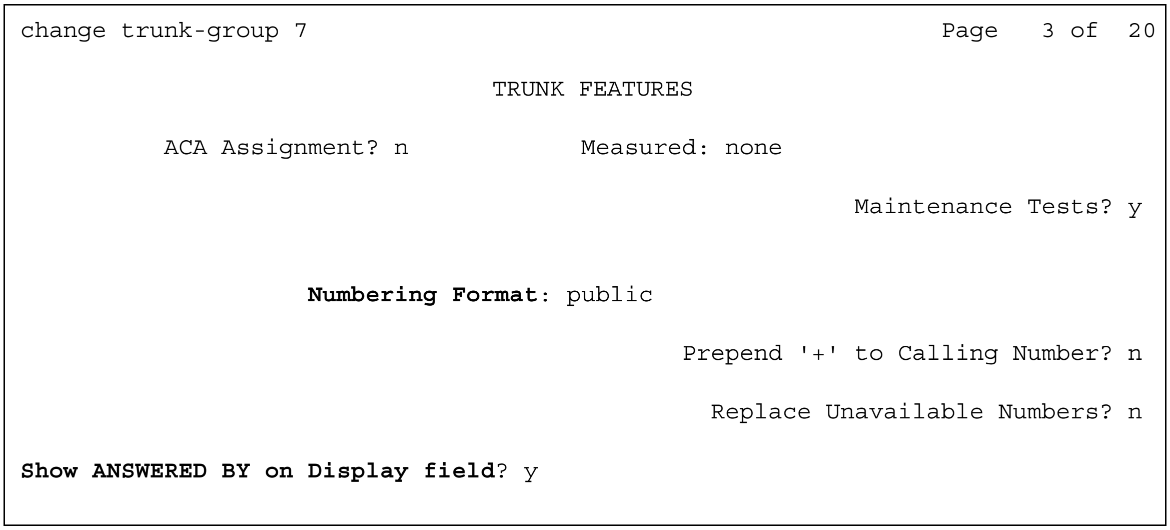
Valid entries	Usage
90 to **1800**	Default 120 seconds. Recommendation for SIP is 1800 seconds. The interval for the session refresh requests is determined through a negotiation mechanism. If a session refresh request is not received before the interval passes, the session terminates. Both endpoints send a BYE, and call state aware proxies can remove any state for the call.

Trunk Group screen, Page 3

The system displays this screen of the Trunk Group screen, the **Trunk Features** screen, shown in Figure 23 when **sip** is the **Group Type** on Trunk Group screen page 1.

Check or administer all of the values on this screen for SIP.

Figure 23: Trunk Group screen, page 3



```
change trunk-group 7                                          Page   3 of  20

                                TRUNK FEATURES

          ACA Assignment? n             Measured: none

                                                       Maintenance Tests? y


                    Numbering Format: public

                                            Prepend '+' to Calling Number? n

                                              Replace Unavailable Numbers? n

Show ANSWERED BY on Display field? y
```

ACA Assignment

In Trunk Group screen, page 3, this field may have a y or n entry.

Valid entries	Usage
y/n	Type **y** if you want Automatic Circuit Assurance (**ACA**) measurements to be taken for this trunk group. If you set this field to **y**, complete the **Service Type** field.The default entry for SIP is **n**.

Measured

In Trunk Group screen, page 3, this field determines if the system will transmit data for this trunk group to the Call Management System (CMS).

You cannot use **internal** and **both** unless either the BCMS (Basic Call Management System) or the **Service Type** field is **y** on the **System-Parameters Customer-Options** screen. If the **ATM** field is set to **y** on the **System-Parameters Customer-Options** screen, this field accepts only **internal** or **none** as values. If this field contains a value other than **internal** or **none** when **ATM** is **y**, the screen displays **none** for the field value.

Valid entries	Usage
internal	Type **internal** if the data can be sent to the BCMS, the VuStats data display, or both.
external	Type **external** to send the data to the CMS.
both	Type **both** to collect data internally and to send it to the Communication Manager.
none	Type **none** if trunk group measurement reports are not required. NOTE: This is the default for SIP trunk groups.

Maintenance Tests

In Trunk Group screen, page 3, the screen displays this field only when the value of the **Group Type** field is **aplt**, **isdn**, **sip**, or **tie**.

Valid entries	Usage
y/n	Type **y** (the default) to run maintenance tests hourly on this trunk group. One or more trunk members must be administered as SIP for this entry to be saved.

Numbering Format

In Trunk Group screen, page 3, the **Numbering Format** field specifies the encoding of Numbering Plan Indicator for identification purposes in the Calling Number, the Connected Number IEs or both, and in the QSIG Party Number. Valid entries are **public**, **unknown**, **private**, and **unk-pvt**.

Valid entries	Usage
Public	Indicates that the number plan according to CCITT Recommendation E.164 is used and that the **Type of Number** is **national**. This is the default entry for SIP trunks.
Unknown	Indicates that the **Numbering Plan Indicator** is **unknown** and that the **Type of Number** is **unknown**.
Private	Indicates the **Numbering Plan Indicator** is **PNP** and the **Type of Number** is determined from the **Private-Numbering** screen.
unk-pvt	Also determines the **Type of Number** from the **Private-Numbering** screen, but the **Numbering Plan Indicator** is **unknown**.

Prepend '+' to Calling Number?

In the Trunk Group screen, page 3, set this field to y if you want to add a plus sign (+) to the beginning of a number to accommodate international calls.

Replace Unavailable Numbers

The system displays this field in the Trunk Group screen, page 3 only when the Group Type field is **isdn** or **sip**. This field dictates whether to replace unavailable numbers with administrable strings for incoming and outgoing calls assigned to the specified trunk group. Administrable strings are located in the System Parameters Features screen, page 1 screen.

This field applies to BRI/PRI and SIP trunks.

Valid entries	Usage
y/n	Type **y** to replace the display of an unavailable number with a phrase, for example, **Private Caller**. The system replaces unavailable numbers regardless of the service type of the trunk. The default for SIP trunks is **n**.

Show ANSWERED BY on Display field

If the outgoing call is over a trunk that might be redirected, some customers would prefer not to see the display message Answered by, but still want to see the connected party number. See Trunk Group screen, page 3.

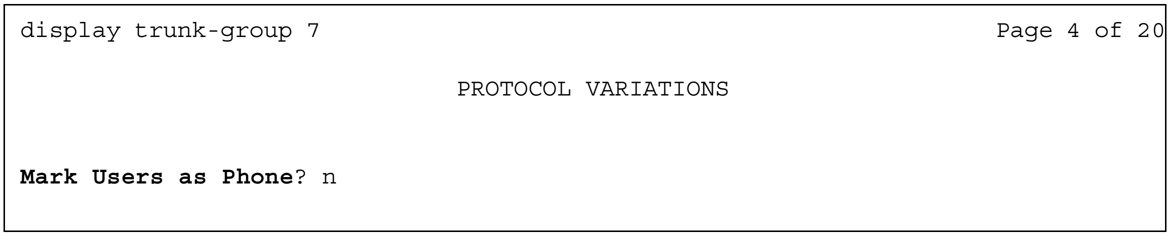
Valid entries	Usage
y/n	Type y to show 'ANSWERED BY' string in the proper language on originator's display when the connected party name is not available. The default for SIP trunks is **y**.

Trunk Group screen, page 4

When the Group Type is **sip**, the system displays the Protocol Variations screen. The system displays this screen for SIP trunks only.

For SIP, set this field to **y** for a particular trunk *only* if a device or network connected to that SIP trunk requires the **user as phone** parameter. Consider the situation of a public network trunking connection to an outside or third party. Set this to **y** for a customer taking the trunk out to a third party.

Figure 24: Protocol Variations screen



```
display trunk-group 7                                      Page 4 of 20

                             PROTOCOL VARIATIONS


Mark Users as Phone? n
```

Mark Users as Phone

Valid entries	Usage
n	Default.
y	URIs in call control signaling messages originated at the gateway are encoded with the "user=phone" parameter. No subscription messages are encoded with the "user=phone" parameter even when the field is set to **y**.

SIP device as an OPS extension

If a 46xx SIP telephone is configured as an OPS extension, then the number of call appearances must be configured in all of these following areas:

1. In `46xxsettings.txt` file or in DHCP scope option: **PHNNUMOFSA** must be set to the number of call appearances.
2. Station screen page 2: set **restrict last appearance = n** (default = y)
3. Station screen, page 3: You must add additional button assignments as 'call appearances' to match the value of PHNNUMOFSA
4. Off-station pbx mapping screen, page 2: the **call limit** must equal the number of call appearances set in **PHNNUMOFSA**.

Appendix A: Requirement specifications

These sections in this appendix explain how SES rules are applied:

- Call processing software

Call processing software

Call processing software is explained in sections covering domains and routing:

- RFC 3325 compliance

RFC 3325 compliance

The material in this book is based on regulatory compliance of RFC 3325 compliance.

Compliance with RFC 3325

The SES proxy complies with RFC 3325, *Network Asserted Identity*.

While RFC 3325 provides for a privacy header, this header does not provide complete anonymity to the user. The privacy header only requires that the p-asserted-identity header be removed from the request.

FNU requirements

The following sections describe how Feature Name URI (FNU) requirements are implemented.

In the column heading, PPM denotes Personal Profile Manager.

- Call Forwarding All Calls FNU on page 100
- Call Forward Busy - No Answer FNU on page 101
- Directed Call Pickup FNU on page 103
- Extended Call Pickup FNU on page 104
- Calling Party Number Block FNU on page 104
- Calling Party Number Unblock FNU on page 105

- Dial Intercom FNU on page 106
- Drop FNU on page 106
- Exclusion FNU on page 107
- Off-PBX Call FNU on page 107
- Last Number Dialed FNU on page 108
- Malicious Call Trace FNU on page 108
- AUDIX One-Step Recording FNU on page 109
- Priority Call FNU on page 109
- Send All Calls FNU on page 110
- Transfer to Voice Mail FNU on page 111
- Whisper Page Activation on page 112

Call Forwarding All Calls FNU

This FNU Activates or deactivates Call Forwarding All Calls.

Case 1—FNU structure where Call Forwarding All Calls, of the endpoint's own (1111) extension:

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-forwarding-all;avaya-cmdestination=
4444444;avaya-cm-action=on SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=call-forwarding-all;avaya-cm-action=on
SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=call-forwarding-all;avaya-cm-action=offSIP/
2.0
```

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Req	No
avaya-cm-destination	Any number within the Communication Manager dial plan, to which this endpoint is being forwarded.	Opt	No

Authorization: This example shows the use of this FNU on the endpoint's own extension. It must be authorized by the extension's class of service. See the next case for how to apply this feature to another extension.

Communication Manager button: call-fwd Ext: (left blank)

Feature package: Yes

SDP required: Only if avaya-cm-action=on and avaya-cm-destination not specified. (if SDP required, line appearance must be requested – otherwise line appearance request will be ignored)

Case 2—FNU structure where Call Forwarding All Calls, of another endpoint's (2222) extension.

```
INVITE
sip:2222@example.com;avaya-cm-fnu=call-forwarding-all;avaya-cmdestinat
ion= 4444444;avaya-cm-action=on SIP/2.0
```

```
INVITE
sip:2222@example.com;avaya-cm-fnu=call-forwarding-all;avaya-cm-action=
on SIP/2.0
```

```
INVITE
sip:2222@example.com;avaya-cm-fnu=call-forwarding-all;avaya-cm-action=
off SIP/2.0
```

Name	Values	Req/Opt	PPM
avaya-cm-destination	Any number within the Communication Manager dial plan, to which this endpoint is being forwarded	Opt	No
avaya-cm-action	on or off	Req	No

Authorization: An endpoint can use this FNU on another extension only if the endpoint has a "call-fwd Ext: 2222" button administered on Communication Manager. Activates or deactivates Call Forwarding All Calls, on the extension specified in the user part of the Request-URI.

Communication Manager button: call-fwd Ext: 2222

Feature package: Yes

SDP required: Only if avaya-cm-action=on and avaya-cm-destination not specified. (if SDP required, line appearance must be requested – otherwise line appearance request will be ignored)

Call Forward Busy - No Answer FNU

Call Forward Busy/Don't Answer activates and deactivates call forwarding for calls when the extension is busy or the user does not answer.

Case 1—FNU structure where Call Forwarding All Calls of the endpoint's own (1111) extension:

```
INVITE
sip:1111@example.com;avaya-cm-fnu=call-forwarding-busy-no-answer;avayacm-dest
ination=4444444;avaya-cm-action=on SIP/2.0
```

```
INVITE
sip:1111@example.com;avaya-cm-fnu=call-forwarding-busy-no-answer;avayacm-acti
on=on SIP/2.0
```

```
INVITE
sip:1111@example.com;avaya-cm-fnu=call-forwarding-busy-no-answer;avayacm-acti
on=off SIP/2.0
```

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Req	No
avaya-cm-destination	Any number within the Communication Manager dial plan, to which this endpoint is being forwarded.	Opt	No

Authorization: This example shows the use of this FNU on the endpoint's own extension. It must be authorized by the extension's class of service. See the next case for how to apply this feature to another extension.

Communication Manager button: cfwd-bsyda Ext: (left blank)

Feature package: Yes

SDP required: Only if avaya-cm-action=on and avaya-cm-destination not specified. (if SDP required, line appearance must be requested, otherwise line appearance request will be ignored)

Case 2—FNU structure where Call Forwarding All Calls of another endpoint's (2222) extension:

```
INVITE
sip:2222@example.com;avaya-cm-fnu=call-forwarding-busy-no-answer;avaya
cm- destination=4444444;avaya-cm-action=on SIP/2.0
```

```
INVITE
sip:2222@example.com;avaya-cm-fnu=call-forwarding-busy-no-answer;avaya
cm- action=on SIP/2.0
```

```
INVITE
sip:2222@example.com;avaya-cm-fnu=call-forwarding-busy-no-answer;avaya
cm- action=off SIP/2.0
```

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Req	No
avaya-cm-destination	Any number within the Communication Manager dial plan, to which this endpoint is being forwarded.	Opt	No

Authorization: An endpoint can use this FNU on another extension only if the endpoint has a “cfwd-bsyda Ext: 2222” button administered on Communication Manager.

Description: Call Forward Busy/Don’t Answer activates and deactivates call forwarding for calls when the extension is busy or the user does not answer, on the extension specified in the user part of the Request-URI.

CM button: cfwd-bsyda Ext: 2222

Feature package: Yes

SDP required: Only if avaya-cm-action=on and avaya-cm-destination not specified. (if SDP required, line appearance must be requested, otherwise line appearance request will be ignored).

Directed Call Pickup FNU

Directed Call Pickup allows the user to answer a call ringing at another extension without having to be a member of a pickup group.

Directed Call Pickup FNU Structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-directed;avaya-cmextension=3333
SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-directed SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-extension	The Communication Manager extension where the call is alerting.	Opt	No

Authorization: The endpoints need not be members of a group, but directed call pickup must be authorized by the class of restriction for both endpoints.

Communication Manager button: dir-pkup

Feature package: No

SDP required: Yes

Extended Call Pickup FNU

Extended Group Call Pickup allows a user to answer calls directed to another call pickup group.

Extended Group Call Pickup FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-extended;avaya-cm-pickupnumber=3
SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=call-pickup-extended SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-pickup-number	The pickup number from 1 to 24.	Opt	No

Authorization: The endpoint must be a member of a pickup group, and that pickup group must be a member of an extended pickup group, which must also include the group of the endpoint whose telephone is being picked up.

Communication Manager button: None. Accessed on the Communication Manager only via an FAC.

Feature package: No

SDP required: Yes

Calling Party Number Block FNU

Calling Party Number Block blocks the sending of the calling party number for one call.

Calling Party Number Block FNU structure:

```
INVITE
sip:1111@example.com;avaya-cm-fnu=calling-party-block;avaya-cmdestinat
ion=4444444 SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=calling-party-block SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-destination	Any number within the Communication Manager dial plan to which this call is being directed.	Opt	No

Authorization: None

Communication Manager button: cpn-blk

Feature package: No

SDP required: Yes

Calling Party Number Unblock FNU

Calling Party Number Unblock deactivates calling party number (CPN) blocking and allows the CPN to be sent for a single call.

Calling Party Number Unblock FNU structure:

```
INVITE
sip:1111@example.com;avaya-cm-fnu=calling-party-unblock;avaya-cmdestin
ation=
```

```
4444444 SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=calling-party-unblock SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-destination	Any number within the Communication Manager dial plan to which this call is being directed	Opt	No

Authorization: None

Communication Manager button: cpn-unblk

Feature package: No

SDP required: Yes

Dial Intercom FNU

Dial Intercom places a call to the station associated with the button. The called user receives a unique alerting indication. The endpoint extension and destination extension must be in the same intercom group. This feature is exactly like Automatic Intercom except for the way that the dial code is specified. PPM can provide the dial code for Automatic Intercom, but not for Dial Intercom.

Dial Intercom FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=dial-intercom;avaya-cm-group=9;avayacm-
dial-code=12 SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=dial-intercom;avaya-cm-group=9 SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-group	Any number within the Communication Manager dial Intercom group number from 1 to 32.	Req	Yes
avaya-cm-dial-code	1- or 2-digit number	Opt	No

Authorization: An endpoint can use this FNU for a intercom group that matches an administered Communication Manager button for this extension.

Communication Manager button: dial-icom Grp: 9

Feature package: No

SDP required: Yes

Drop FNU

Drop FNU allows users to drop calls. Users can drop calls from automatic hold or drop the last party they added to a conference call.

Drop FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=drop SIP/2.0
```

Parameters: None

Authorization: None

Communication Manager button: drop

Feature package: No

SDP required: No

Exclusion FNU

Exclusion allows multi-appearance telephone users to keep other users with appearances of the same extension from bridging onto an existing call. If the user activates the Exclusion button while other users are already bridged onto the call, the other users are dropped.

There are two ways to activate Exclusion.

- Manual Exclusion—when the user presses the exclusion button (either during dialing or during the call)
- Automatic Exclusion—as soon during a call, the user presses the exclusion button

Exclusion FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=exclusion
      ;avaya-cm-action=on SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=exclusion
      ;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Opt	No

Authorization: This request always applies to the endpoint’s own extension. Automatic exclusion must be authorized by the extension’s class of service.

Description:

Communication Manager button: exclusion

Feature package: No

SDP required: No

Off-PBX Call FNU

This FNU provides the capability to enable and disable the extending of an EC500 call.

Off-PBX Call FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=off-pbx;avaya-cm-action=on SIP/2.0
INVITE sip:1111@example.com;avaya-cm-fnu=off-pbx;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Req	No

Authorization: This request always applies to the endpoint's own extension.

Communication Manager button: ec500

Feature package: Yes

SDP required: No

Last Number Dialed FNU

Last Number Dialed (redial) originates a call to the number last dialed by the station.

Last Number Dialed FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=last-number-dialed SIP/2.0
```

Parameters: None

Authorization: None

Communication Manager button: last-numb

Feature package: No

SDP required: Yes

Malicious Call Trace FNU

Malicious Call Trace Activation sends a message to the MCT control extensions stating that the user wants to trace a malicious call. MCT activation also starts recording the call, if the system has a MCT voice recorder.

Malicious Call Trace FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=mct SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=mct-cancel SIP/2.0
```

Parameters: None

Authorization: Must be authorized by the endpoint's class of restriction

Communication Manager button: mct-act (to activate). Only an FAC to cancel.

Feature package: No

SDP required: No

AUDIX One-Step Recording FNU

This feature allows a station user to start and end the recording of an in-progress conversation using the AUDIX system recording facility. Note that avaya-cm-extension is optional when avaya-cm-action is "off" (because a station can only have one of these buttons).

AUDIX One-Step Recording

```
INVITE sip:1111@example.com; avaya-cm-fnu=one-touch-recording;
avaya-cmextension=3333;avaya-cm-action=on SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=one-touch-recording;avaya-cmaction=off SIP/
2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Req	No
avaya-cm-extension	The Communication Manager extension of an AUDIX hunt group	Req	Yes

Authorization: An endpoint can use this FNU on another extension only if the endpoint has a Communication Manager button audix-rec button with a matching extension.

Communication Manager button: audix-rec Ext: 3333

Feature package: No

SDP required: No

Priority Call FNU

Priority Calling allows a user to place priority calls or change an existing call to a priority call.

Priority Call FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=priority-call;avaya-cm-destination=4444444
SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=priority-call SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-destination	Any number within the Communication Manager dial plan, to which this call is being directed	Opt	No

Authorization: None

Communication Manager button: priority

Feature package: No

SDP required: Yes

Send All Calls FNU

Send All Calls allows users to temporarily direct all incoming calls to coverage regardless of the assigned call-coverage redirection criteria.

Send All Calls of the endpoint’s own (1111) extension FNU structure

```
INVITE sip:1111@example.com;avaya-cm-fnu=sac;avaya-cm-action=on SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=sac;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Req	No

Authorization: This example shows the use of this FNU on the endpoint’s own extension. No authorization is required. See the next case for how to apply this feature to another extension.

Communication Manager button: send-calls Ext: (left blank)

Feature package: Yes

SDP required: No

Send All Calls of another endpoint's (2222) extension FNU structure

```
INVITE sip:2222@example.com;avaya-cm-fnu=sac;avaya-cm-action=on SIP/2.0
```

```
INVITE sip:2222@example.com;avaya-cm-fnu=sac;avaya-cm-action=off SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-action	on or off	Req	No

Authorization: An endpoint can use this FNU on another extension only if the endpoint has a "send-calls Ext: 2222" button administered on Communication Manager.

Description: Applied to another extension.

Communication Manager button: send-calls Ext: 2222

Feature package: Yes

SDP required: No

Transfer to Voice Mail FNU

Transfer to Voice Mail FNU allows coverage to transfer the caller to the original call recipient's AUDIX mail where the caller can leave a message.

Transfer to Voice Mail FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=transfer-to-voicemail SIP/2.0
```

Parameters: None

Authorization: None

Communication Manager button: None. Accessed on the Communication Manager only by an FAC.

Feature package: No

SDP required: No

Whisper Page Activation

Whisper Page Activation allows a user to make and receive whisper pages. A whisper page is an announcement sent to another extension that is active on a call where only the person on the extension hears the announcement. Other parties on the call cannot hear the announcement.

Whisper Page Activation FNU structure:

```
INVITE sip:1111@example.com;avaya-cm-fnu=whisper-page;avaya-cm-extension=3333 SIP/2.0
```

```
INVITE sip:1111@example.com;avaya-cm-fnu=whisper-page SIP/2.0
```

Parameters:

Name	Values	Req/Opt	PPM
avaya-cm-extension	The Communication Manager extension to which you want to whisper	Req	No

Authorization: The user must have a class of restriction (COR) that allows intra-switch calling to use whisper paging, and the extension to which you are whispering must not have blocked whispers.

Communication Manager button: whisp-act

Feature package: No

SDP required: Yes

Appendix B: Terminal requirements and features

This appendix has two major sections that discuss Communication Manager's terminal requirements, features, and feature interactions with respect to SIP.

- Terminals

Terminals

Avaya CM OPTIM requirements

Outgoing From header

OPTIM formats the outgoing **From: URI** field in the call that leaves the switch from a non-SIP telephone to a SIP telephone. The From header is as follows:

Display parameter followed administered digits at authoritative URI. The digits depend on the configuration set option calling number style. There are two choices: **network** and **PBX**. **PBX** is the station extension. **Network** is the network station modified by either the public or the private number table. The domain is taken from the Network Regions screen. If this is not administered the default is `anonymous.unknown.domain`. For an incoming ISDN call terminating to an OPTIM OPS station, the display information comes from the display IE and the handle is from the calling number. The domain is as above.

Glossary

A

access code A dial code of 1 to 3 digits that activates a feature, cancels a feature, or accesses an outgoing trunk.

Access Security Gateway (ASG) A software module that secures Avaya Global Services log in accounts on many Avaya servers. Each login attempt on these accounts is met with a one-time challenge string that must be answered with the correct one-time response.

American National Standards Institute (ANSI) A professional technical association that supports standards for transmission, protocol, and high-level languages, and that represents the U.S. in the International Organization for Standards. ANSI standards are for voluntary use in the U.S.

Avaya Communication Manager An open, scalable, highly reliable, and secure telephony application. Communication Manager provides user functionality and system management functionality, intelligent call routing, application integration and extensibility, and enterprise communications networking.

B

bearer channel (B-channel) A 64-kbps channel or a 56-kbps channel that carries a variety of digital information streams. A B-channel carries voice at 64 kbps, data at up to 64 kbps, WebLM voice encoded at 64 kbps, and voice at less than 64 kbps, alone or combined. See also data channel (D-channel).

bus A multiconductor electrical path that transfers information over a common connection from any of several sources to any of several destinations. *See also* packet bus; time-division multiplex (TDM) bus.

C

Call Detail Recording (CDR) A file that uses software and hardware to record call data. CDR was formerly called Station Message Detail Recording (SMDR). *See also* Call Detail Recording utility (CDRU).

Call Detail Recording utility (CDRU) Software that collects, stores, filters, and provides output of call detail records. *See also* Call Detail Recording (CDR).

carrier An enclosed shelf that contains vertical slots that hold circuit packs.

CCRON Coverage of calls redirected off-network.

central office (CO) Telephone switching equipment that provides local telephone service and access to toll facilities for long distance calling.

channel (1) A circuit-switched call. (2) A communications path that transmits voice and data. (3) In WebLM transmission, all the contiguous time slots or noncontiguous time slots that are necessary to support a call. For example, an H0-channel uses six 64-kbps time slots. (4) A digital signal-0 (DS0) on a T1 facility or an E1 facility that is not specifically associated with a logical circuit-switched call. *See also* data channel (D-channel).

circuit (1) An arrangement of electrical elements through which electric current flows. (2) A channel or a transmission path between two or more points.

circuit pack A circuit card on which electrical circuits are printed, and integrated circuit (IC) chips and electrical components are installed. A circuit pack is installed in a SSH carrier. One example is the TN2302.

Class of Restriction (COR) A feature that allows up to 96 classes of call-origination restrictions and call-termination restrictions for telephones, telephone groups, data modules, and trunk groups. *See also* Class of Service (COS).

Class of Service (COS) A feature that uses a number to specify whether telephone users can activate the Automatic Callback (ACB), Call Forwarding All Calls, Data Privacy, or Priority Calling features. *See also* Class of Restriction (COR).

CCITT Comitte Consultatif International Telephonique et Telegraphique. *See* International Telecommunications Union (ITU).

communications system A software-controlled processor complex that interprets dial pulses, tones, and keyboard characters, and makes the proper connections within the system and externally. The communications system consists of a digital computer, software, storage devices, and carriers, with special hardware to perform the connections. A communications system provides communications services for the telephones on customer premises and the data terminals on customer premises, including access to public networks and Point-to-Point Protocol (PPP)s. *See also* SSH.

Controlled Local Area Network (CLAN) circuit pack A circuit pack (TN799B) in an Avaya DEFINITY port network (PN) that provides TCP/IP connectivity to adjuncts over Ethernet or Point-to-Point Protocol (PPP). The CLAN circuit pack serves as the network interface for a DEFINITY server. The CLAN terminates IP (TCP and UDP), and relays those sockets and connections up to the Avaya DEFINITY server.

CPN Called-party number

CPN/BN Calling-party number/billing number

CSP Cellular Service Provider.

customer-premises equipment (CPE) Equipment that is connected to the telephone network, and that resides on a customer site. CPE can include telephones, modems, fax machines, video conferencing devices, switches, and so on.

D

data channel (D-channel) A 16-kbps channel or a 64-kbps channel that carries signaling information or data on an Integrated Services Digital Network Basic Rate Interface (ISDN-BRI) or Integrated Services Digital Network Primary Rate Interface (ISDN-PRI). *See also* bearer channel (B-channel).

data communications equipment (DCE) Equipment on the network side of a communications link that makes the binary serial data from the source or the transmitter compatible with the communications channel. DCE is usually a modem, a data module, or a packet assembly/disassembly (PAD).

data module An interconnection device between a Basic Rate Interface (BRI) or a Digital Communications Protocol (DCP) interface of the SSH, and the data terminal equipment (DTE) or data channel (D-channel).

data terminal An input/output (I/O) device that has either switched access or direct access to a host computer or to a processor interface.

data terminal equipment (DTE) Equipment that comprises the endpoints in a connection over a data circuit. In a connection between a data terminal and a host, the terminal, the host, and the associated modems or data modules comprise the DTE.

digital The representation of information by discrete steps. Compare with *analog*.

Digital Communications Protocol (DCP) A proprietary protocol that transmits both digitized voice and digitized data over the same communications link. A DCP link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels, and thus two telephones or data modules. The I1 channel is the DCP channel that is assigned on the first page of the 8411 Station screen. The I2 channel is the DCP channel that is assigned on the analog adjunct page of the 8411 Station screen, or on the data module page.

dual-tone multifrequency (DTMF) The touchtone signals used for in-band telephone signaling.

Dynamic Host Configuration Protocol (DHCP) An IETF protocol (RFCs 951, 1534, 1542, 2131, and 2132) that assigns IP addresses dynamically from a pool of addresses instead of statically.

E

extension A number from 1 digit to 5 digits that routes calls through a communications system. With a Uniform Dial Plan (UDP) or a main-satellite dialing plan, extensions also route calls through a Point-to-Point Protocol (PPP).

F

FNU Feature Name URI

FTP File transfer protocol.

feature A specifically defined function or service that the system provides

H

H.323 An International Telecommunications Union (ITU) standard for switched multimedia communication between a LAN-based multimedia endpoint and a gatekeeper.

host computer A computer that is connected to a network, and that processes data from data-entry devices.

I

IE *See* information element (IE).

IEEE *See* Institute of Electrical and Electronics Engineers (IEEE).

IETF *See* Internet Engineering Task Force (IETF).

IM Instant Messaging. The instant-messaging client software required for the Avaya Communication Manager release 2.0 or later is a version of the Avaya IP Softphone R5 and later, and the SIP Softphone R2 and later.

information element (IE) The name for the data fields within an Integrated Services Digital Network (ISDN) Layer 3 message.

IP interface A CLAN, ethernet processor interface, or procr that lets the server connect using internet protocol.

Institute of Electrical and Electronics Engineers (IEEE) An organization that produces standards for local area network (LAN) equipment.

Integrated Services Digital Network (ISDN) A public network or a Point-to-Point Protocol (PPP) that provides end-to-end digital communications for all services to which users have access. An ISDN uses a limited set of standard multipurpose user-network interfaces that are defined by the CCITT. Through internationally accepted standard interfaces, an ISDN provides digital circuit switching communications or packet switching communications within the network. An ISDN provides links to other ISDNs to provide national digital communications and international digital communications. *See also* Integrated Services Digital Network Basic Rate Interface (ISDN-BRI); Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Basic Rate Interface (ISDN-BRI) The interface between a communications system and terminal that includes two 64-kbps bearer channel (B-channel)s for transmitting voice or data, and one 16-kbps data channel (D-channel) for transmitting associated B-channel call control and out-of-band signaling information. ISDN-BRI also includes 48 kbps for transmitting framing and D-channel contention information, for a total interface speed of 192 kbps. ISDN-BRI serves ISDN terminals and digital terminals that are fitted with ISDN terminal adapters. *See also* Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Primary Rate Interface (ISDN-PRI)

The interface between multiple communications systems that in North America includes 24 64-kbps channels that correspond to the North American digital signal-level 1 (DS1) standard rate of 1.544 Mbps. The most common arrangement of channels in ISDN-PRI is 23 64-kbps bearer channel (B-channel)s for transmitting voice and data, and one 64-kbps data channel (D-channel) for transmitting associated B-channel call control and out-of-band signaling information. With nonfacility-associated signaling (NFAS), ISDN-PRI can include 24 B-channels and no D-channel. *See also* Integrated Services Digital Network (ISDN); Integrated Services Digital Network Basic Rate Interface (ISDN-BRI).

International Organization for Standards

A worldwide federation of standards bodies who issue International Standards for technological, scientific, intellectual, and economic activity. The federation is called *ISO*, and the US representative to the federation is the American National Standards Institute (ANSI).

International Telecommunications Union (ITU)

An international organization that sets universal standards for data communications, including Integrated Services Digital Network (ISDN). ITU was formerly known as International Telegraph and Telephone Consultative Committee (CCITT).

International Telegraph and Telephone Consultative Committee

See International Telecommunications Union (ITU).

Internet Engineering Task Force (IETF)

One of two technical working bodies of the Internet Activities Board. The IETF develops new Transmission Control Protocol (TCP)/Internet Protocol (IP) (for example, TCP/IP) standards for the Internet.

Internet Protocol (IP)

A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (OSI) model. IP protocol is used for Internet addressing and routing packets over multiple narrowbands to a final destination. IP protocol works in conjunction with Transmission Control Protocol (TCP), and is usually identified as TCP/IP.

L

local area network (LAN)

A networking arrangement that is designed for a limited geographical area. Generally, a LAN is limited in range to a maximum of 6.2 miles, and provides high-speed carrier service with low error rates. Common configurations include daisy chain, star (including circuit-switched), ring, and bus.

M

MAC address (or MAC name)

A 48-bit number, uniquely identifying and programmed into each network interface card or device.

media server interface A CLAN card in a media server.

MWI messaging waiting indication.

N

NAME1 Legacy name, Latin characters, usually displayable, for example Eurofont and Kanafont encoding.

NAME2 UTF-8 encoding. Used for multibyte character sets such as Chinese ideograms Hiragana, Katakana, and Hangul

narrowband A circuit-switched call at a data rate of 64 kbps or less. All switch calls that are not WebLM are considered to be narrowband. Compare with wide band.

network A series of points, nodes, or stations that are connected by communications channels.

network region Network Region is a flexible administrative concept. A network region is an attribute associated with Communication Manager resources. It is used for among other things resource allocation and security.

For example, when an H.323, or SIP, endpoint requires a Gateway Resource to set up a talk path with a non-IP endpoint like a DCP telephone, Communication Manager checks the network region parameter to attempt to get that gateway resource from the same Network Region, that is, as near to the endpoint as possible, to minimize trunk usage and delay.

node A switching point or a control point for a network. Nodes are either tandem or terminal. Tandem nodes receive signals, and pass the signals on. Terminal nodes originate a transmission path, or terminate a transmission path.

nonce Random value sent in a communications protocol exchange, often used to detect replay attacks.

This specifically refers to the use of random information inserted in a challenge for SIP digest authentication. The algorithms are essentially the same as for HTTP, and are described in RFC2617.

O

OATS Origination and terminating signaling. Formerly known as origination-based call flow or W call flow. In a call flow diagram, describes the direction, initiation, and termination of signaling

off-PBX station (OPS) A telephone that Avaya Communication Manager does not control, such as a cellular telephone or the home telephone of a user. The features of Communication Manager can be extended to an OPS through switch administration by associating the extension of the office telephone with the off-site telephone.

OPS Outboard Proxy SIP.

Open Systems Interconnect (OSI) A system of seven independent communication protocols defined by the International Organization for Standards or ISO. Each of the seven layers enhances the communications services of the layer below, and shields the layer above from the implementation details of the lower layer. In theory, this structure can be used to build communications systems from independently developed layers.

origination-based call flow See OATS.

O/S Operating System.

P

packet A group of bits that is used in packet switching and that is transmitted as a discrete unit. A packet includes a message element and a control information element (IE). The message element is the data. The control IE is the header. In each packet, the message element and the control IE are arranged in a specified format.

packet assembly/disassembly (PAD) The process of packetizing control data and user data from a transmitting device before the data is forwarded through the packet network.The receiving device disassembles the packets, removes the control data, and then reassembles the packets, thus reconstituting the user data in its original form.

packet bus A bus with a wide bandwidth that transmits packets.

packet switching A data-transmission technique that segments and routes user information in discrete data envelopes that are called *packets*. Control information for routing, sequencing, and error checking is appended to each packet. With packet switching, a channel is occupied only during the transmission of a packet. On completion of the transmission, the channel is made available for the transfer of other packets.

PBX private branch exchange. *See* SSH.

Plain Old Telephone Service (POTS) Basic voice communications with standard, single-line phones accessing the public switched telephone network (PSTN).

PPM Personal Profile Manager (PPM) is a centralized repository of personalized data, such as contact lists or access control lists. PPM provides a Web Services interface that allows a client, such as a SIP telephone or SIP Softphone, to download a particular user's profile, thus allowing the user the mobility to move around to different devices but maintain access to the user's unique information.

As an example, a user might log in one day at a telephone at a service desk, and then the next from a Softphone while working from home. In each case, the user's personal profile would appear at each of those devices.

Point-to-Point Protocol (PPP) A standard (largely replacing SLIP) allowing a computer to use TCP/IP with a regular telephone line.

port A data-transmission access point or voice-transmission access point on a device that is used for communicating with other devices.

private network A network exclusively for the telecommunications needs of a particular customer.

processor ethernet A logical connection between the server itself and a network interface card. The way this connection is administered in Communication Manager determines what type of traffic the NIC allows.

procr See processor ethernet.

protocol A set of conventions or rules that governs the format and the timing of message exchanges. A protocol controls error correction and the movement of data.

proxy trust domain Includes those SIP servers and gateways, but not endpoints with identities administered on the SES.

public network A network to which all customers have open access for local calling and long distance calling.

public switched telephone network (PSTN) The public worldwide voice telephone network.

R

RAS Remote Access Server (or in Microsoft Windows operating systems, Remote Access Service).

Real Time Transfer Protocol (RTP) An Internet Engineering Task Force (IETF) protocol (RFC 1889) that addresses the problems that occur when video and other exchanges with real-time properties are delivered over a local area network (LAN) that is designed for data. RTP gives higher priority to video and other real-time interactive exchanges than to connectionless data.

RFA Remote Feature Activation is a web-based application which is used to obtain Avaya authentication and licensing files.

RFC Request for Comments designates Internet Engineering Task Force (IETF) standards that are drafts.

RNIS Remote Network Implementation Services is a contract installation services group within Avaya Inc.

RPM RedHat Package Manager

RSA Remote Supervisor Adapter

RTC Real Time Communication

RTCP Real Time Control Protocol

S

S8400 A hardware platform for use as a media server that is a single module. The S8400 uses a flash drive, and the SAMP functionality is on the board. No separate chassis is required.

S8500 A hardware platform from the IBM x305 series. This machine uses an RSA for a remote maintenance board.

S8500B A hardware platform from the IBM x306 series. This machine uses a SAMP for a remote maintenance board.

SCCAN The Seamless Converged Communications Across Networks (SCCAN) solution offers voice and data access from a single SCCAN handset integrated with a desk phone across the corporate Wireless Local Area Network (WLAN) and public Global System for Mobile communication (GSM) and cellular networks.

Session Initiated Protocol (SIP) A signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. SIP initiates call setup, routing, authentication, and other feature messages to endpoints within an IP domain. *See also* H.323; Voice over IP (VoIP).

SIP Enablement Services SES. SIP Enablement Services is the new name for Converged Communication Server.

SSH Secure SHell is a protocol for secure remote login and other secure network services over an insecure network. It provides for server authentication, and data integrity with perfect port-forwarding secrecy.

SSL Secure Socket Layer.

subscriber A subscriber is one of the following: a SIP Enablement Services host or other SIP node, a SIP user (per Contact), or a Media Server (running Avaya Communication Manager 2.0 or later).

switch Any kind of telephone switching system. *See also* communications system.

T

TAC trunk-access code

TCP *See* Transmission Control Protocol (TCP).

TCP/IP *See* Internet Protocol (IP). *See also* Transmission Control Protocol (TCP).

tie trunk A telecommunications channel that directly connects two private switching systems.

time-division multiplex (TDM) bus A bus that is time-shared regularly by pre allocating short time slots to each transmitter. In a SSH, all Plain Old Telephone Service (POTS) circuits are connected to the time-division multiplex (TDM) bus, and any port can send a signal to any other port. *See also* time-division multiplexing (TDM).

time-division multiplexing (TDM) A form of multiplexing that divides a transmission channel into successive time slots. *See also* time-division multiplex (TDM) bus.

time slot

In the SSH, a time slot refers to either a digital signal level-0 (DS0) on a T1 facility or an E1 facility, or a 64-kbps unit on the time-division multiplex (TDM) bus or fiber connection between port networks (PNs) that is structured as 8 bits every 125 microseconds.

Transmission Control Protocol (TCP)

A connection-oriented transport-layer protocol, IETF STD 7. RFC 793, that governs the exchange of sequential data. Whereas the Internet Protocol (IP) deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data, and also guarantees that packets are delivered in the same order in which the packets are sent.

Transport Layer Security (TLS)

An IETF standard (RFC 2246) to supersede Netscapes' Secure Socket Layer (SSL) and provide host-to-host data connections with encryption and certification at the transport layer.

trunk

A dedicated communications channel between two communications systems or central office (CO)s.

trunk access code (TAC)

A dial access code used to access a specific trunk.

trunk group

Telecommunications channels that are assigned as a group for certain functions, and that can be used interchangeably between two communications systems or central office (CO)s.

W

W call flow

See OATS.

Index